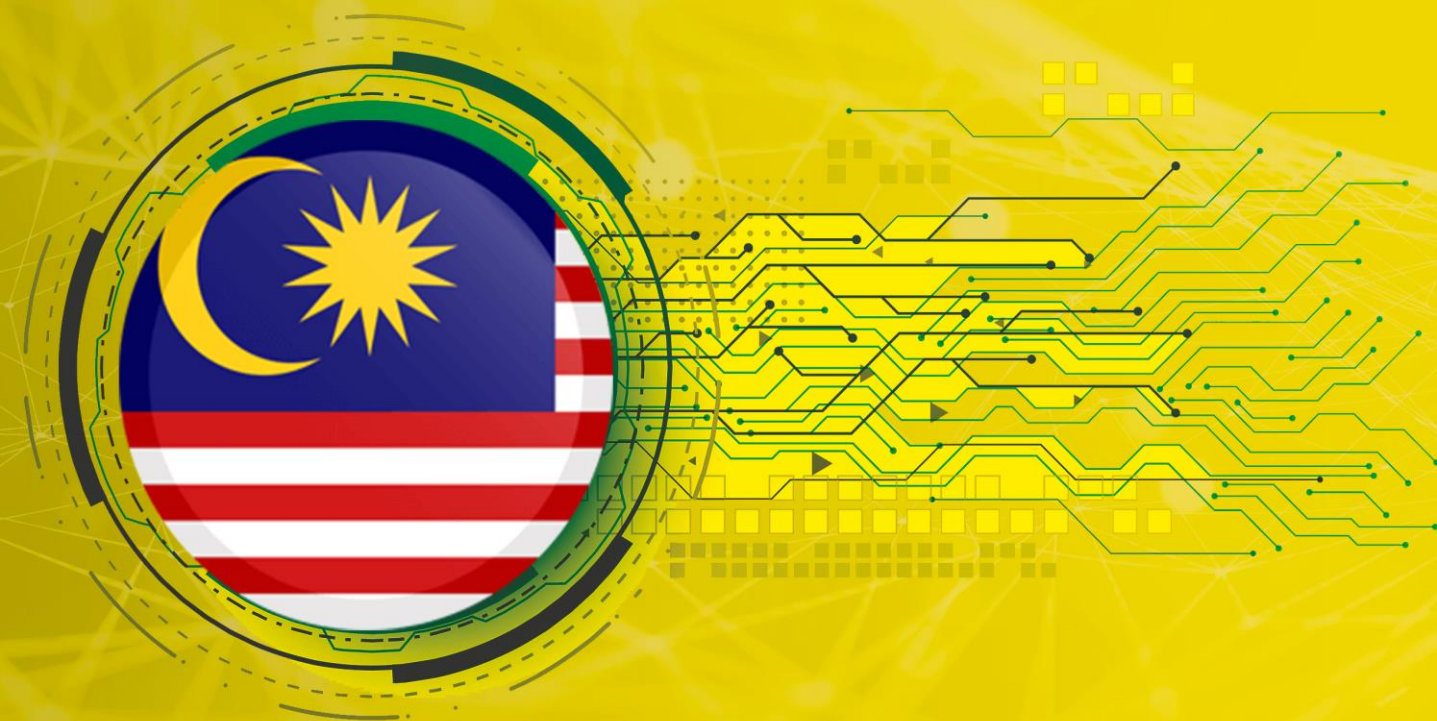
جمهوری اسلامی ایران
شورای عالی فضای مجازی
مرکز ملی فضای مجازی

گزارش سریع ۱۴

حکمرانی فضای مجازی در کشورهای جهان

مالـزی



www.majazi.ir

بسم الله الرحمن الرحیم

جمهوری اسلامی ایران
مرکز ملی فضای مجازی

حکمرانی فضای مجازی در کشور مالزی

گزارش سریع (۱۴)
بهمن ماه ۱۳۹۸

تهیه شده در: پژوهشگاه فضای مجازی- گروه مطالعات فرهنگی و اجتماعی
تهیه‌کننده: عباس قنبری باغستان (عضو هیات علمی گروه ارتباطات دانشگاه تهران)
ناظر علمی: امیررضا باقرپورشیرازی

نشانی: تهران، میدان آرژانتین، خیابان بیهقی، نبش خیابان ۱۶ غربی، پلاک ۲۰، کدپستی ۱۵۱۵۶۷۴۳۱۱
شماره تماس: ۸۶۱۲۱۰۶۱ http://www.majazi.ir

گزارش سریع که با عنوان Rapid Report شناخته می‌شود، نوعی گزارش کوتاه است که صرفاً برای اطلاع کلی از موضوع یا پدیده‌ای خاص در بازه زمانی محدود تهیه می‌شود. هدف عمده چنین گزارش‌هایی، ایجاد تصویری اجمالی برای آشنایی ابتدایی سیاست‌گذاران و برنامه‌ریزان در موضوعات مورد علاقه آنان است.

چکیده

هنگامی‌که از حکمرانی فضای مجازی سخن می‌گوییم، دست‌کم سه مفهوم را می‌توانیم مورد نظر قرار دهیم:

۱) حکمرانی از طریق فضای مجازی: حکومت‌ها برخی از وظایف حاکمیتی خود را از طریق فضای مجازی انجام می‌دهند. برای مثال، خدمات دولتی از طریق اینترنت ارائه می‌شود. مفهوم «دولت الکترونیک» در این حوزه جای می‌گیرد.

۲) حکمرانی در فضای مجازی: حکومت‌ها سعی می‌کنند حاکمیت سرزمینی خود را در فضای مجازی بازتعریف و اِعمال کنند. برای مثال، آن‌ها دامنه‌های ملی تعریف می‌کنند، در پی امنیت سایبری شهروندان خود هستند، جرائم را به حوزه سایبری بسط می‌دهند یا آن‌ها را با توجه به فضای سایبری تعدیل می‌کنند.

۳) حکمرانی بر فضای مجازی: حکومت‌ها سعی می‌کنند سیاست‌هایی را برای شکل‌دادن به فعالیت‌ها در فضای مجازی تدوین و اجرا کنند، رویه‌های عمل قانونی و مشروع را در فضای مجازی تعیین کنند و روابط میان بازیگران و گروه‌های اجتماعی مختلف را تنظیم کنند.

سلسله گزارش‌های «حکمرانی فضای مجازی در کشورهای جهان» تلاش می‌کند تا «ساختار، مدل و سناریو حکمرانی فضای مجازی»، «اسناد سیاستی و قوانین فضای مجازی»، «مهمترین نهادها و شرکت‌های ملی فضای مجازی» و «مهمترین اقدامات حاکمیتی فضای مجازی» این کشورها را مورد بررسی قرار دهد. در این گزارش، به حکمرانی فضای مجازی در کشور مالزی خواهیم پرداخت.

واژگان کلیدی

حکمرانی فضای مجازی، مالزی، برنامه چشم‌انداز ۲۰۲۰ مالزی، شورای ملی آی.تی مالزی، سیاست امنیت سایبری ملی، نظارت و فیلترینگ، قانون ضد-اخبار جعلی

فهرست مطالب

مقدمه

«حکمرانی سایبری» به عنوان مقوله‌ای نسبتاً جدید کمتر از یک دهه است که وارد ادبیات سیاسی و روابط بین‌الملل کشورها شده است. ظهور فناوری‌های مربوط به فضای سایبری باعث ایجاد تحول در مفهوم «قدرت» و تغییر در موازنه «منابع» آن شده و به این ترتیب با ظهور بازیگران جدید عرصه در قدرت و حاکمیت، نوع حکمرانی کشورها نیز دچار دگرگونی فراوان شده است.

در مطالعه مواجهه کشورها با "فضای سایبری" و ارزیابی نوع حکمرانی‌شان در این عرصه جدید، اگرچه رویکردهای مختلفی قابل شناسایی است، اما وجه غالب و عمده آن‌ها به دلیل فقدان "اِشراف راهبردی" در حوزه فناوری، "امنیت و دفاع سایبری" است که براساس آن، اطمینان از "امنیت" در فضای سایبری به عنوان مرکز ثقل هرگونه سیاست‌گذاری و برنامه‌ریزی هدف‌گذاری شده است. "امنیت سایبری" به این اعتبار خود یک مقوله دوجهی است که یک بُعد آن جنبه "دفاعی" داشته، به معنای مقابله با حملات سایبری، جاسوسی سایبری و جرایم سایبری است، و بُعد دیگر آن جنبه "ایجابی" دارد و به معنای ظرفیت‌سازی و ایجاد اعتماد در حوزه سایبری در راستای اهداف توسعه‌ای است.

هدف از تدوین این گزارش، مطالعه نحوه مواجهه مالزی با "فضای سایبری" و نوع حکمرانی این کشور در این فضای جدید و نوظهور می‌باشد. مطالعه "حکمرانی سایبری" در مالزی و نوع مواجهه آن با "فضای سایبری" با هدف استفاده از تجربه این کشور از این منظر حایز اهمیت است که مالزی توانسته به عنوان یک کشور در حال توسعه، الگوی موفقی از توسعه بومی ارایه دهد که مورد توجه جامعه جهانی نیز قرار گرفته، به‌طوری که به عنوان یکی از مهم‌ترین دستاوردهای آن، بانک جهانی اخیراً اعلام کرده که مالزی با توجه به روند رشد خود تا سال ۲۰۲۴ به جمع کشورهای "پُردرآمد" خواهد پیوست. ضمن آن‌که مالزی به عنوان یک کشور اسلامی، قرابت‌ها و مشترکات فرهنگی، دینی و تاریخی زیادی با ایران دارد و از این‌رو می‌توان در مقایسه با سایر کشورهای توسعه‌یافته و در حال توسعه، از الگوی آن برای هرگونه سیاست‌گذاری و یا برنامه‌ریزی در این زمینه استفاده کرد.

مطالعه نحوه مواجهه مالزی با فضای سایبری و نوع حکمرانی این کشور در فضای سایبری به‌طور وثیقی با برنامه‌های توسعه این کشور، به خصوص "چشم انداز ۲۰۲۰" مالزی و به تبع آن "زیرساخت اطلاعات ملی" این کشور عجین است. از این‌رو، قبل از هرچیزی مداقه در برنامه "چشم انداز ۲۰۲۰" مالزی، شناخت ابعاد مختلف آن و از همه مهم‌تر، جایگاهی که برای فناوری ارتباطات و اطلاعات در این "چشم انداز" تصور شده است، ضروری می‌باشد.

برنامه چشم‌انداز ۲۰۲۰ مالزی: زمینه‌های ورود به سیاست‌گذاری فضای مجازی

آغاز برنامه توسعه مالزی موسوم به "چشم‌انداز ۲۰۲۰" در سال ۱۹۹۱ که براساس آن این کشور می‌بایست از اقتصاد کشاورزی به اقتصاد "دانش بنیان" گذار کند و هم‌زمانی آن با ساخت "سوپر کریدور مولتی مدیای"[۱]این کشور توسط ماهاتیر محمد، نخست وزیر وقت، را می‌توان سرآغاز سیاست‌گذاری و برنامه‌ریزی در ارتباط با فضای سایبری (با تأکید بر تهدیدها، فرصت‌ها، چالش‌ها و آسیب‌های مرتبط با آن) دانست.

اساس برنامه "چشم‌انداز ۲۰۲۰" مالزی بر استفاده گسترده از ظرفیت‌های "ارتباطاتی و اطلاعاتی" به عنوان ابزاری برای توسعه استوار است که منجر به استفاده گسترده از فناوری‌های نوین در بخش صنعت، بخش خصوصی، بخش عمومی و سایر حوزه‌های در سطح وسیع می‌شود. براساس برنامه چشم‌انداز ۲۰۲۰، دولت به طور کلی ۱۰ حوزه را به عنوان "حوزه‌های کلیدی" در سطح ملی انتخاب کرده که عمده تلاش‌ها، برنامه‌ریزی‌ها، سیاست‌گذاری‌ها و سرمایه‌گذاری‌ها برای تحقق اهداف چشم‌انداز ۲۰۲۰ در این ۱۰ حوزه متمرکز می‌شوند. این ده حوزه در واقع ده حوزه کلیدی هستند که "زیرساخت اطلاعاتی ملی"[۲]این کشور را تشکیل می‌دهند.

ده حوزه کلیدی در "زیرساخت اطلاعاتی ملی" کشور مالزی

ده حوزه کلیدی در "زیرساخت اطلاعاتی ملی" مالزی، حوزه‌ها (فیزیکی-مجازی)، سیستم‌ها و کارکردهایی هستند که برای توسعه ملی مالزی حیاتی هستند و هرگونه نقصان، اختلال و یا تخریب آن تأثیر شگرفی در ۱-اقتصاد ملی، ۲-ایماژ ملی[۳] ۳-دفاع و امنیت ملی، ۴-ظرفیت‌های کارکردی دولت و نیز ۵- سلامت و امنیت عمومی این کشور خواهد داشت. همچنین متناظر با

---

[۱] Multimedia Super Corridor

[۲] Critical National Information Infrastructure

[۳] National Image

این ۱۰ حوزه، ۱۰ نهاد و سازمان مسئول، که عمدتاً وزارتخانه‌های این کشور می‌باشند، نیز به عنوان نهادها و سازمان‌های مسئول و متولی این ۱۰ حوزه معرفی شده‌اند که باید براساس چشم‌انداز ۲۰۲۰ این کشور، برای دستیابی به اهداف از پیش تعیین‌شده سیاست‌گذاری، برنامه‌ریزی و اقدام نمایند. این حوزه‌های کلیدی موسوم به "۱۰ حوزه زیرساخت اطلاعاتی ملی" به همراه نهادها/سازمان‌های متولی هر کدام در جدول و شکل شماره ۱ نمایش داده شده‌اند که شامل موارد ذیل می شوند:

جدول ۱: ده حوزه کلیدی در زیرساخت اطلاعاتی کشور مالزی به تفکیک نهادها/سازمان‌های مذکور

ردیف	حوزه زیرساخت	نهادهای مسئول
۱	دفاع و امنیت ملی	وزارت دفاع (نظامیان) و وزارت کشور (پلیس)
۲	بانکداری و فایننس	وزارت فایننس، بانک مرکزی و کمیسیون امنیت
۳	اطلاعات و ارتباطات	وزارت اطلاعات، ارتباطات و فرهنگ و کمیسیون مولتی‌مدیا
۴	انرژی	کمیسیون انرژی، شرکت ملی نفت و شرکت ملی برق
۵	حمل‌ونقل	وزارت حمل‌ونقل
۶	آب	کمیسیون ملی خدمات آب
۷	سلامت و بهداشت	وزارت بهداشت
۸	دولت	دپارتمان برنامه‌ریزی مدیریت، مدرن سازی و اجرایی (دفتر نخست‌وزیر)
۹	خدمات اضطراری	وزارت مسکن و شهرسازی
۱۰	غذا و کشاورزی	وزارت کشاورزی

با توجه به تمرکز بسیار زیاد این چشم‌انداز ۲۰۲۰ مالزی بر استفاده از فناوری آی.تی و حرکت بخش‌های صنعت، خصوصی، عمومی و دیگر حوزه‌ها به سوی "سیستم اطلاعات دیجیتال"[۱]، بدیهی است که دولت مالزی هم‌زمان با تغییر و تحولات فناوری‌های نوین، سیاست‌ها و

[۱] Digital Information System

استراتژی‌های نوینی برای صیانت و اطمینان از کارایی و عملکرد ده حوزه کلیدی "زیرساخت اطلاعات ملی" این کشور اتخاذ نماید.

شکل ۱: ده حوزه کلیدی در زیرساخت اطلاعاتی کشور مالزی به تفکیک نهادها/سازمان‌های مذکور

تدوین «سیا ست امنیت سایبری ملی»[۱] سناریویی برای حکمرانی فضای مجازی

تدوین سند "سیاست امنیت سایبری ملی"، اولین و مهم‌ترین نماد مواجهه دولت مالزی با فضای نسبتاً جدید "سایبری" بود که سابقه آن به اوایل قرن ۲۱ برمی‌گردد. از ابتدا، برنامه‌ریزی برای تدوین "سیاست امنیت سایبری ملی " به وزارت علوم، فناوری و نوآوری[۲] مالزی محول شده است. با توجه به این مسئولیت، این وزارتخانه در سال ۲۰۰۵ کار تحقیقاتی در این زمینه

---

[۱] National Cyber Security Policy

[۲] Ministry of Science, Technology & Innovation (MOSTI)

را آغاز و پس از یکسال مطالعه، تحقیق و بررسی، پیشنهادات خود را در قالب سند "سیاست امنیت سایبری ملی" در ماه می ۲۰۰۶، به تأیید "شورای ملی آی.تی."[1]مالزی رساند.

هدف راهبردی در سند "سیاست امنیت سایبری ملی" مالزی عبارت است از این که "ده حوزه کلیدی زیرساخت اطلاعاتی ملی این کشور باید "امن"، "منعطف" و "خوداتکاء" باشد. این وضعیت با ترویج فرهنگ "امنیت"[2]در جامعه، منجر به ثبات، توسعه و نیز ایجاد رفاه و ثروت در جامعه خواهد شد". "سیاست امنیت سایبری ملی" مالزی براساس پنج محور اصلی تدوین شده است که به شرح ذیل می باشد:

۱-مقررات‌گذاری و قانون‌گذاری: اینکه در این کشور باید قوانین مُکفی (اعم از اجرایی و نیز حقوقی و قضایی) برای رسیدگی به امور مربوط به فناوری‌های نوین اطلاعاتی و ارتباطی از جمله در حوزه سایبر وجود داشته باشد.

۲- فناوری و نوآوری: این کشور باید به جدیدترین فناوری‌ها و نوآوری‌های ارتباطی دسترسی داشته باشد.

۳-همکاری بخش خصوصی-دولتی: برای تحقق اهداف توسعه‌ای، همکاری و همراهی بخش خصوصی با دولت ضروری است.

۴-سازماندهی (ساختار/سازماندهی): حکمرانی در حوزه فناوری و نوآوری به خصوص در حوزه سایبری، نیازمند سازماندهی براساس تفکیک وظایف و مسئولیت‌ها است.

جدول ۱: هشت حوزه اصلی "سیاست امنیت سایبری ملی" مالزی به تفکیک نهادهای متولی و وظایف

ردیف	حوزه[3]	پیشران‌ها	وظیفه
۱	حکمرانی مؤثر	وزارت علوم، فناوری و نوآوری	تأسیس مرکز ملی هماهنگی اطلاعاتی-امنیتی

[1] National IT Council (NITC)
[2] Culture of Security
[3] Thrust

۲	چارچوب حقوقی و قانونی	دادگاه عمومی (مدعی‌العموم)[1]	پیگرد قضایی و قانونی جرائم سایبری
۳	چارچوب فناوری امنیت سایبری	وزارت علوم، فناوری و نوآوری	صدور گواهی/تأییدیه برای مدیریت امنیت-اطلاعات و تضمین آن
۴	فرهنگ "امنیت" و ظرفیت‌سازی	وزارت علوم، فناوری و نوآوری	کاهش تعداد حوادث امنیتی-اطلاعاتی از طریق افزایش آگاهی‌ها و مهارت‌ها
۵	تحقیق و توسعه به‌سوی خوداتکایی[2]	وزارت علوم، فناوری و نوآوری	پذیرش و استفاده از محصولات داخلی مربوط به حوزه اطلاعاتی-امنیتی
۶	انطباق و اجرا[3]	وزارت اطلاعات، ارتباطات و فرهنگ	اطمینان از اجرای و انطباق قوانین مربوطه در ۱۰ حوزه کلیدی زیرساخت اطلاعاتی ملی
۷	آمادگی اضطراری[4] در حوزه امنیت سایبری	شورای امنیت ملی	ایجاد انعطاف و آمادگی در ۱۰ حوزه کلیدی زیرساخت اطلاعاتی ملی در مقابل جرائم سایبری، تروریسم، جنگ اطلاعاتی و ...
۸	همکاری‌های بین‌المللی	وزارت اطلاعات، ارتباطات و فرهنگ	برند سازی در سطح بین‌المللی از طریق اقدامات خلاقانه در حمایت، تقویت و امنیت ۱۰ حوزه کلیدی زیرساخت اطلاعاتی ملی

۵-همکاری‌های بین‌المللی: یک از اهداف مالزی در هر زمینه‌ای، تبدیل‌شدن به الگو و برند جهانی است. حوزه سایبری نیز از این امر مستثنی نیست. مالزی با هدف تبدیل‌شدن به الگو در مقیاس منطقه‌ای و بین‌المللی باید از طریق همکاری نزدیک با کشورهای جهان به خصوص در قالب سازمان‌های مهم بین‌المللی همچون سازمان ملل و سازمان کنفرانس اسلامی نقش

[1] Attorney General's Chambers
[2] Self-Reliance
[3] Compliance & Enforcement
[4] Emergency Readiness

مشارکت‌جویانه همراه با رهبری داشته باشد (National Cyber Security Policy: The Way Forward, 2006).

در "سیاست امنیت سایبری ملی" مالزی، همچنین هشت حوزه اصلی (پیشرو) تعریف شده و متناظر با هر حوزه، یکی از وزاتخانه‌ها، نهادها و یا سازمان‌های این کشور به عنوان "پیشران"، مسئول آن حوزه تعیین شده که باید نسبت به تأمین پنج محور فوق در حوزه مسئولیتی خود اطمینان حاصل کند. براین اساس، اگر نسبت به تأمین مؤثر شرایط هشت حوزه فوق در هر یک از ده حوزه کلیدی "زیرساخت اطلاعاتی ملی" این کشور اطمینان حاصل شود، مالزی به هدف راهبردی سایبری خود دست یافته است. در واقع، وظیفه و مسئولیت هریک از نهادهای ذکر شده در جدول شماره ۲ به عنوان "پیشران"، اطمینان از تحقق شرایط و وظایفی است که در سند "سیاست امنیت سایبری ملی" به آن اشاره شده است. تحقق این شرایط و وظایف، در واقع تضمین‌کننده تحقق اهداف مندرج در چشم‌انداز ۲۰۲۰ این کشور می‌باشد.

هشت حوزه پیشرو در "سیاست امنیت سایبری ملی"

همان‌طور که قبلاً نیز گفته شد، "سیاست امنیت سایبری ملی" مالزی مبتنی بر هشت حوزه می‌باشد که در هر حوزه، یکی از نهادها یا سازمان‌های مالزیایی به عنوان مسئول آن حوزه، اهداف و وظایفی را بر عهده دارند. این هشت حوزه عبارتند از:

۱-حکمرانی مؤثر: این حوزه در واقع به معنای به‌رسمیت‌شناختنِ "وابستگی متقابل" هر ده حوزه کلیدی زیرساخت اطلاعات ملی در کشور مالزی است. هدف از تعیین این حوزه عبارت است از: ۱-متمرکز ساختن هرگونه اقدام و فعالیت در ارتباط با "امنیت سایبری ملی"، ۲- تشویق و ترغیب همکاری مؤثر بین بخش‌های عمومی، دولتی و خصوصی، و ۳-ایجاد بستر تبادل اطلاعات در حوزه‌های مربوط.

۲-چارچوب حقوقی و قانونی: این حوزه بیشتر به موضوعات حقوقی و قضایی مربوط به فضای سایبری پرداخته و هدف از آن، تأمین یک "نظام قانونی، حقوقی و قضایی" مُکفی برای حوزه سایبری است که همیشه در حال تغییر و تحول می‌باشد. به این اعتبار، وجود قوانین و نیز مقررات‌گذاری لازم برای "ایجاد اطمینان" و "اعتمادسازی" در ده حوزه کلیدی "زیرساخت اطلاعات ملی" بسیار ضروری است. اهداف جزئی‌تر این حوزه عبارت است از: ۱-مطالعه و ارزیابی

قوانین سایبری مالزی، ۲-پیگیری و رصد طبیعت سیال و متغیر تهدیدات امنیت سایبری مالزی، ۳-پایه‌گذاری برنامه‌های مدرن در زمینه "ظرفیت‌سازی" در حوزه سایبری برای مؤسسات و آژانس‌های ملی مجری قانون، ۴-اطمینان از اینکه تمامی قوانین اجرایی داخلی هسمو و هماهنگ با قوانین، معاهدات و کنوانسیون‌های بین‌المللی هستند.

۳-چارچوب فناوری امنیت سایبری: به صورت کلی، دستورالعمل‌ها و کتابچه‌های زیادی در بین مردم در ارتباط با "امنیت سایبری" وجود دارد. با این‌حال بسیاری از آن‌ها ناقص و دربردارنده همه دستورالعمل‌ها و راهنمایی‌های لازم نیستند. هدف از این حوزه که زیر نظر وزارت علوم، فناوری و نوآوری مالزی می‌باشد، تدوین و توسعه یک چارچوب فناوری امنیت سایبری است که "نیازها و لوازم امنیت اطلاعات" را مشخص می‌سازد، عناصر ده حوزه کلیدی "زیرساخت اطلاعاتی ملی" را کنترل و رصد می‌کند و سیستم‌ها و محصولات مربوط به "امنیت اطلاعات" را ارزیابی، تأیید و اجرایی می‌کند. زمانی که صحبت از "امنیت اطلاعات" می‌شود، مسائل مهمی همچون "مدیریت اطلاعات" و "کنترل فنی و عملیاتی" و ... برجسته می‌شود که نقش مهمی در امنیت سایبری دارند.

۴-فرهنگ "امنیت سایبری": این حوزه بیش از هرچیز بر ابعاد انسانی سیاست‌گذاری در حوزه سایبری متمرکز می‌باشد. اهداف دقیق این حوزه عبارتند از: ۱- توسعه، ترویج و حفظ فرهنگ ملی "امنیت"، ۲-استانداردسازی و هماهنگی برنامه‌های آموزشی وآگاهی‌بخشی در زمینه "امنیت اطلاعات" در هر ده حوزه کلیدی "زیرساخت اطلاعات ملی" کشور و ۳-پایه‌گذاری یک مکانیسم مؤثر در زمینه توزیع و نشر سواد و دانش "امنیت اطلاعات" در سطح ملی و ۴-تعیین حداقل نیازمندی‌ها و کیفیت لازم برای کارشناسان و متخصصان امنیت اطلاعات. در این خصوص، باید تأکید نمود که توسعه و ترویج فرهنگ "امنیت سایبری" مستلزم رهبری و نیز مشارکت نهادها و سازمان‌های متعدد است. برای همین هدف، باید یک نقشه راه استراتژیک با مشارکت همه وزارتخانه‌ها و نهادهای درگیر برنامه‌ریزی و مدیریت شود.

۵-"تحقیق و توسعه" به سوی خوداتکایی: برای دستیابی به خوداتکایی، در تمامی ده حوزه کلیدی "زیرساخت اطلاعات ملی" باید یک چارچوب "تحقیق و توسعه" یکپارچه تهیه و به اجرا گذاشته شود که مهم‌ترین هدف آن "به سوی خوداتکایی" باشد. اهداف دقیق این حوزه عبارتند

از: ۱-مدیریت، فرمول‌بندی و اولویت‌سنجی فعالیت‌های "تحقیق و توسعه" در زمینه امنیت سایبری، ۲- تقویت و گسترش محققین حوزه "امنیت اطلاعات"، ۳- ترویج توسعه و تجاری‌سازی مالکیت معنوی، فناوری و نوآوری از طریق "تحقیق و توسعه"، ۴-کمک در تقویت و توسعه صنعت "امنیت اطلاعات".

۶-انطباق و اجرا: با توجه به اینکه عمده رگولاتوری‌های ارتباطی و اطلاعتی مالزی (شامل کمیسیون ارتباطات و مولتی مدیا، مخابرات مالزی، شبکه‌های تلفن همراه و ...) زیر نظر وزارت اطلاعات، ارتباطات و فرهنگ این کشور است، حوزه "انطباق و اجرا" به این وزارتخانه واگذار شده است. اهداف دقیق این حوزه به عبارتند از: ۱-استانداردسازی برای سیستم‌های "امنیت اطلاعات" تمامی عناصر ده حوزه‌های کلیدی "زیرساخت اطلاعات ملی"، ۲- تقویت، نظارت و اطمینان از اِعمال و اجرای این استانداردها، ۳-توسعه و تدوین یک چارچوب ارزیابی از "ریسک و خطرات امنیت اطلاعات" در این کشور. برای دستیابی به این اهداف، وزارت اطلاعات، ارتباطات و فرهنگ مالزی مکانیسم‌ها کنترلی مستقل و نیز حسابرسی‌ها و ممیزی‌های امنیتی متناوبی دارد که در ارتباط با دستگاه‌ها و نهادهای ده حوزه کلیدی "زیرساخت اطلاعات ملی" این کشور اِعمال می‌شود. این حسابرسی‌ها و ممیزی‌ها باعث شناسایی نقاط ضعف و حوزه‌هایی می‌شوند که به لحاظ "امنیت سایبری" نیاز به کمک دارند.

۷-آمادگی اضطراری در حوزه امنیت سایبری: تیم واکنش اضطراری رایانه‌ای[۱] ابزار مهمی برای کاهش تهدیدات سایبری در این کشور است. این تیم که در کمپانی "امنیت سایبری مالزی" مستقر است، به طور مداوم تهدیدات سایبری در این کشور را مانیتور و رصد می‌کند. اهداف دقیق‌تر این حوزه عبارتند از: ۱-تقویت تیم واکنش اضطراری رایانه‌ای، ۲-توسعه مکانیسم شناسایی و گزارش‌دهی حوادث مربوط با "امنیت اطلاعات"، ۳-تشویق هر ده حوزه کلیدی "زیرساخت اطلاعات ملی" این کشور به اینکه همواره حوادث مربوط به "امنیت اطلاعات" خود را مانیتور و رصد کنند، ۴- انتشار به موقع توصیه‌ها و مشاوره‌ها در زمینه تهدیدات سایبری و

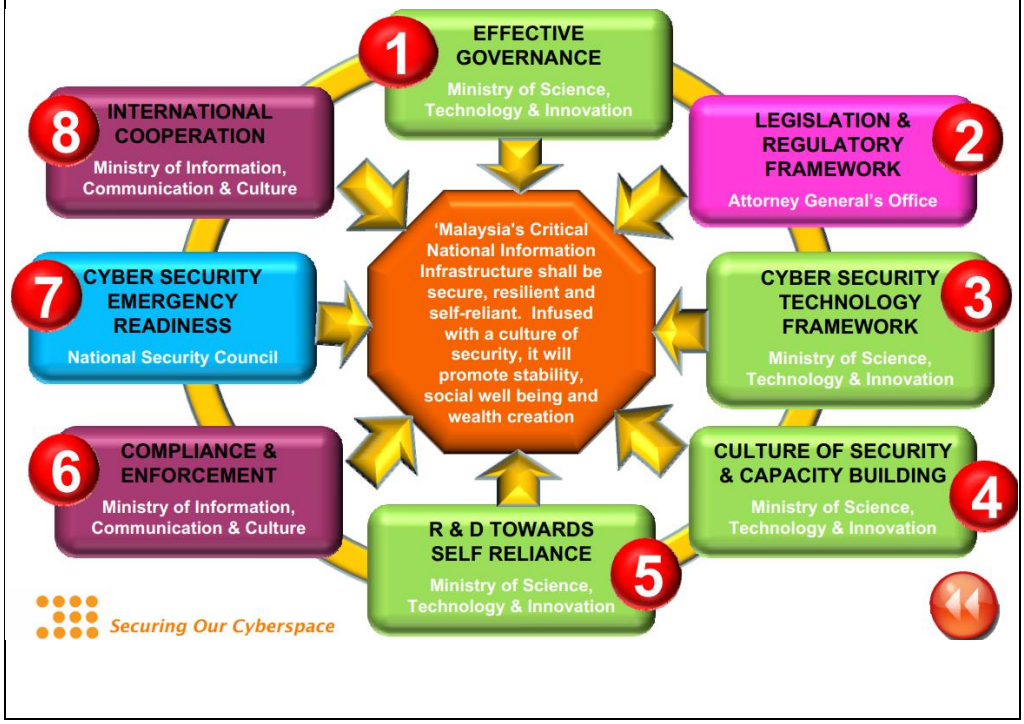
---

[۱] The Computer Emergency Response Teams (CERT)

۵- تشویق هر ده حوزه کلیدی "زیرساخت اطلاعات ملی" این کشور به اینکه به صورت دوره‌ای برنامه‌های ارزیابی در زمینه "امنیت اطلاعات" داشته باشند.

۸-همکاری‌های بین المللی: دامنه فعالیت‌های سایبری محدود به مرزهای جغرافیایی کشورها نیست. از این‌رو موفقیت در زمینه اقدامات و فعالیت‌های مرتبط با امنیت سایبری منوط به همکاری بین‌المللی است. تبادل دانش و اطلاعات، بحث و ارزیابی چالش‌های پیش‌رو با سایر کشورها، فراگیری تجارب کشورهای دیگر و جلوگبری از تکرار اشتباهات دیگران و از همه مهم‌تر، کمک و همفکری در جهت‌دهی به سیاست‌های بین‌المللی در حوزه سایبری به مالزی کمک خواهد کرد تا بهتر بتواند هر ده حوزه کلیدی "زیرساخت اطلاعات ملی" این کشور را مصون نگه دارد. اهداف دقیق‌تر این حوزه عبارتند از: ۱-تشویق به مشارکت فعالانه در تمامی نهادها و سازمان‌های بین‌المللی مرتبط با "امنیت اطلاعات"، حضور در پانل‌ها و نیز آژانس‌های چند ملیتی مربوط، ۲- تشویق به مشارکت فعالانه در تمامی کنفرانس ها، فروم‌ها، و رویدادهای علمی بین‌المللی مرتبط با "امنیت اطلاعات"، ۳- تقویت جایگاه استراتژیک مالزی در زمینه "امنیت اطلاعات" از طریق میزبانی از کنفرانس‌ها و سمینارهای علمی بین‌المللی در زمینه "امنیت اطلاعات"(Mohd Shamir b Hashim, 2011).

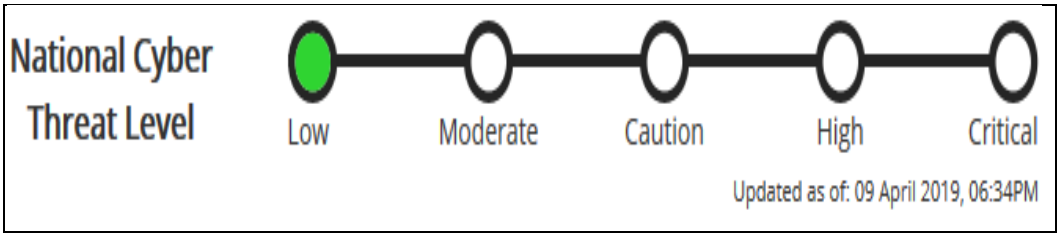
شکل ۱: حوزه‌های اصلی سیاست امنیت سایبری ملی مالزی به تفکیک نهادهای متولی و وظایف



ساختار سیاست‌گذاری و اجرایی "حوزه سایبری" در کشور مالزی

پس از تدوین سند "سیاست امنیت سایبری ملی"، متولی اصلی حوزه سایبری در کشور مالزی بر عهده وزارت علوم، فناوری و نوآوری این کشور گذاشته شده بود. با این‌حال، در بازنگری سال ۲۰۱۰ و با توجه به تغییر وظایف و مسئولیت‌های وزارتخانه‌ها، ساختار جدیدی ارایه شد.

شکل ۱: ارزیابی دولت مالزی از وضعیت امنیت سایبری این کشور (آپریل ۲۰۱۹)



در ساختار جدید حوزه سایبری کشور مالزی و براساس حوزه اول (حکمرانی مؤثر) که به وزارت علوم، فناوری و نوآوری واگذار شده، راه‌اندازی "مرکز ملی هماهنگی اطلاعاتی-امنیتی"

پیش‌بینی شده است. در چارچوب فعالیت‌های این مرکز، ساختار ذیل پیش‌بینی شده است (National Cyber Security Policy: The Way Forward, 2006).

شورای ملی آی.تی مالزی[۱]

این شورا در سال دوبار تشکیل جلسه می‌دهد. اعضای اصلی آن نخست وزیر (به عنوان رئیس)، معاون نخست وزیر و وزیر علوم، فناوری و نوآوری (دبیر شورا) می‌باشد. در این شورا همچنین نمایندگانی از بخش خصوصی، بخش دولتی و نهادهای مدنی حضور دارند. در ذیل این شورا، سه کمیته دیگر شامل : ۱- کمیته مشورتی امنیت سایبری ملی مالزی،[۲] ۲- کمیته هماهنگی امنیت سایبری ملی مالزی،[۳] ۳- کمیته ملی مدیریت بحران سایبری،[۴] ۴- کارگروه ملی مدیریت بحران سایبری[۵] و ۵- کارگروه بحران سایبری[۶] فعال هستند که اعضای آن ترکیبی از نمایندگان ۱۸ نهاد/سازمان فعالی در حوزه سایبری در کشور مالزی از قبیل، وزارت خارجه، وزارت کشور، وزارت دفاع، کمیسیون ارتباطات، شورای امنیت ملی، کمیسیون انرژی، کمیسیون ارتباطات و ... می‌باشد. شکل شماره ۴، ساختار حکمرانی سایبری در کشور مالزی را همراه با جزئیات آن نشان می‌دهد.

---

[۱] National IT Council (NITC)

[۲] National Cyber Security Advisory Committee (NaCSAC)

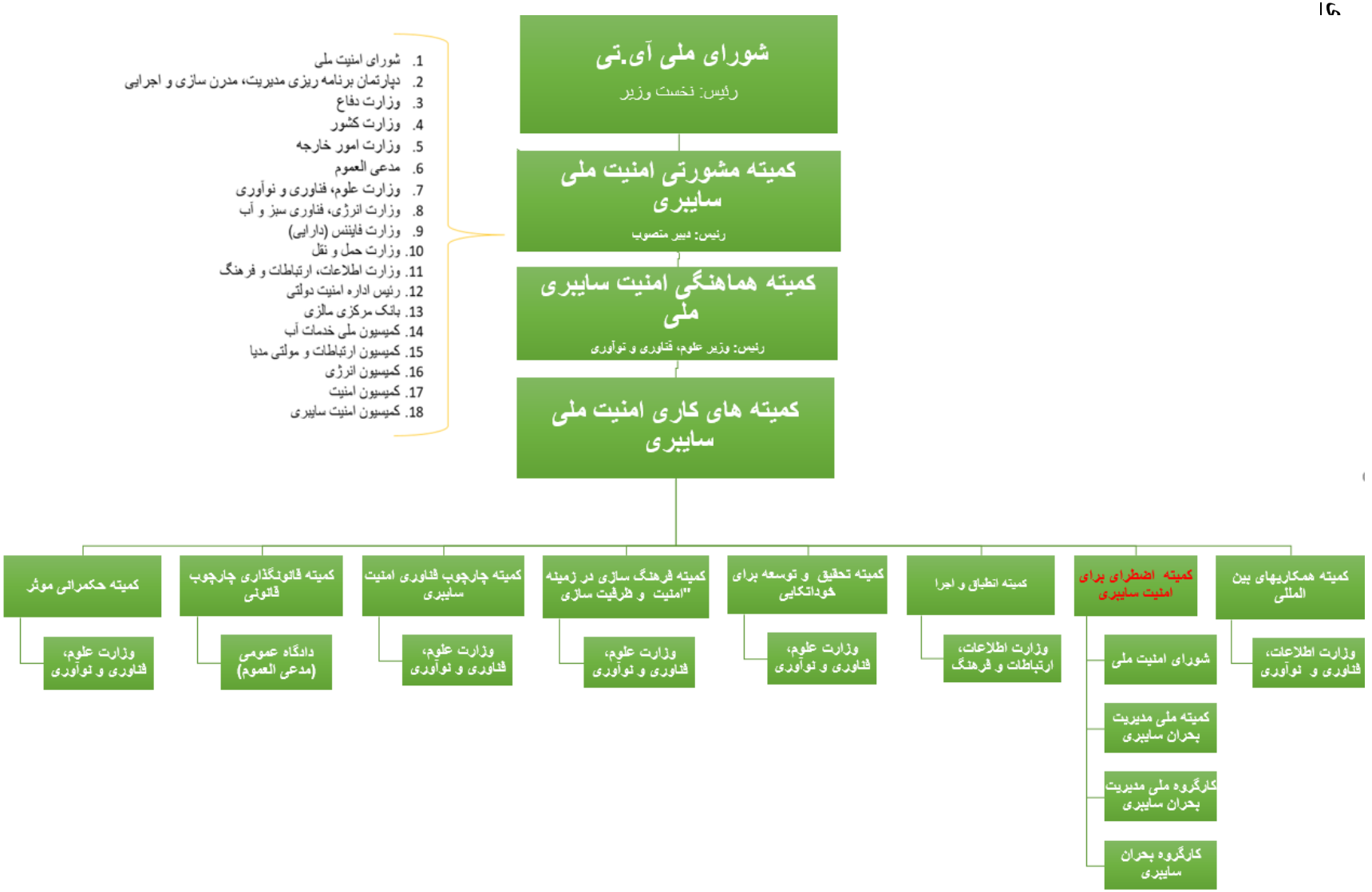
[۳] National Cyber Security Coordination Committee (NC3)

[۴] National Cyber Crisis Management Committee (NCCMC)

[۵] National Cyber Crisis Management Working Group

[۶] Cyber Crisis Working Group

شکل ۲: ساختار حکمرانی سایبری در کشور مالزی



نهادها و سازمان‌های اجرایی ویژه در ارتباط با حوزه سایبری در مالزی

برای رسیدگی به امور مربوط به حوزه سایبری، اعم از آموزش، خدمات و تحقیقات مربوط به جرایم این حوزه، نهادها و سازمان‌هایی در کشور مالزی فعال هستند که اهم آن‌ها به شرح ذیل می‌باشند:

۱-کمپانی "امنیت سایبری مالزی"[1]

این کمپانی در دو سطح دولتی و خصوصی فعال می‌باشد و فعالیت‌های آن زیر نظر وزارت علوم، فناوری و نوآوری می‌باشد. وظیفه این کمپانی دریافت گزارش‌ها در ارتباط با حوادث سایبری (Cyber۹۹۹) در این کشور می‌باشد. برگزاری دوره‌های آموزشی در زمینه فضای سایبری و ارایه خدمات فنی مهندسی به شرکت‌ها و کمپانی‌های بخش‌های مختلف دولتی، خصوصی و صنعتی از دیگر وظایف این کمپانی می‌باشد. این کمپانی دارای سه پلتفرم برای ارایه خدمات می‌باشد:

الف-فضای سایبری مصون:[2] این دپارتمان نقش پیشگیرانه داشته و مسئول آموزش و افزایش آگاهی عموم مردم در مورد مسائل فنی و موضوعات اجتماعی است که افراد در استفاده از اینترنت، به ویژه در مورد خطرات و پیامدهای منفی آن، با آن‌ها روبرو هستند.

ب- **کلنیک‌های سایبری:**[3] این کلینیک‌ها مسئول ارایه خدمات فوری و اضطراری به کاربران به هنگام مواجهه با تهدیدات و یا حملات سایبری می‌باشد. بازیابی داده‌ها، پایش داده‌ها و ... از جمله مهم‌ترین خدمات مربوط به این کلینیک‌ها می‌باشد.

---

[1] Cybersecurity Malaysia
[2] CyberSAFE
[3] CyberSecurity Clinics

ج-توسعه حرفه‌ای امنیت سایبری[۱]: این یک پلتفرم جدید است که وظیفه آن تربیت کارشناسان "امنیت اطلاعات"، ترویج تبادل دانش و آخرین دستاوردها با پیشگامان بخش صنعت و دانشگاه‌ها و همچنین تلاس برای توسعه همکاری‌های ملی، منطقه‌ای و بین‌المللی در حوزه فضای سایبری می‌باشد.

جدول ۰۱: نهادها و اقدامات حاکمیتی فضای مجازی در مالزی

	نمونه نهادهای ملی	نمونه شرکت‌های ملی
حاکمیت امنیتی	کمپانی "امنیت سایبری مالزی" Malaysia Cyber Security	• این کمپانی در دو سطح دولتی و خصوصی فعال می باشد و فعالیت های آن زیر نظر وزارت علوم، فناوری و نوآوری می باشد. این کمپانی دارای سه پلتفرم برای ارایه خدمات می باشد: **الف-فضای سایبری مصون:** این دپارتمان نقش پیشگیرانه داشته و مسئول آموزش و افزایش آگاهی عموم مردم در مورد مسائل فنی و موضوعات اجتماعی دارد که افراد در استفاده از اینترنت، به ویژه در مورد خطرات و پیامدهای منفی آن، با آنها روبرو هستند. ب- **کلنیک های سایبری:** این کلینیک ها مسئول ارایه خدمات فوری و اضطراری به کاربران به هنگام مواجهه با تهدیدات و با حملات سایبری می باشد. بازیابی داده ها، پایش داده ها، و ... از جمله مهمترین خدمات مربوط به این کلینیک ها می باشد. **ج-توسعه حرفه ای امنیت سایبری:** این یک پلتفرم جدید است که وظیفه این تربیت کارشناسان "امنیت اطلاعات"، ترویج تبادل دانش و آخرین دستاوردها با پیشگامان بخش صنعت و دانشگاه ها و همچنین تلاس برای توسعه همکاری های ملی، منطقه ای و بین المللی در حوزه فضای سایبری می باشد.
حاکمیت حقوقی و قضایی	۱-شعبه تحقیقات مولتی مدیا و جرایم سایبری ۲-دادگاه ویژه سایبری	۱-این شعبه زیر نظر دپارتمان تحقیقات مربوط به جرایم تجاری پلیس فدرال (پادشاهی) مالزی می باشد. تحقیقات اولیه در ارتباط با جرایم سایبری توسط این شعبه انجام می شود. این شعبه همچنین وظیفه رصد تمامی فعالیت های جاری و سایری در فضای سایبری از جمله فعالیت های مرتبط با گروه های تروریستی، فعالیت های خلاف امنیت پادشاهی مالزی، فعالیت ها و تبلیغات خلاف دین اسلام و ... بر عهده دارد. ۲-این دادگاه جزئی از دادگاه فدرال مالزی است که در سال ۲۰۱۶ راه اندازی شد و ویژه رسیدگی قضایی به جرایم مربوط به حوزه سایبری از جمله حمله هکری، قماربازی آنلاین، پورنوگرافی آنلاین، جاسوسی و ... می باشد.
حاکمیت فنی	تیم پاسخ اضطراری کامپیوتری	• فعالیت این تیم در سطح ملی است و همراه از طریق Cyber999 در دسترس است. این تیم برای حوادث کامپیوتری به خصوص آلوده شدن آنها به ویروس، از کار افتادن شبکه های کامپیوتری و ... در شرایط فوریت و اضطرار می باشد.

[۱] Cyber Security Professional Development (CyberGuru)

۲-شعبه تحقیقات مولتی مدیا و جرایم سایبری[۱]

این شعبه زیر نظر دپارتمان تحقیقات مربوط به جرایم تجاری پلیس فدرال (پادشاهی) مالزی می باشد. تحقیقات اولیه در ارتباط با جرایم سایبری توسط این شعبه انجام می‌شود. این شعبه همچنین وظیفه رصد تمامی فعالیت‌های جاری را در فضای سایبری از جمله فعالیت‌های مرتبط با گروه‌های تروریستی، فعالیت‌های خلاف امنیت پادشاهی مالزی، فعالیت‌ها و تبلیغات خلاف دین اسلام و ... بر عهده دارد.

۳-دادگاه ویژه سایبری[۲]

این دادگاه جزئی از دادگاه فدرال مالزی است که در سال ۲۰۱۶ راه‌اندازی شد و ویژه رسیدگی قضایی به جرایم مربوط به حوزه سایبری از جمله حمله هکری، قماربازی آنلاین، پورنوگرافی آنلاین، جاسوسی و ... می‌باشد.

۴-تیم پاسخ اضطراری کامپیوتری[۳]

فعالیت این تیم در سطح ملی است و همواره از طریق Cyber999 در دسترس است. این تیم برای حوادث کامپیوتری به خصوص آلوده‌شدن آن‌ها به ویروس، از کار افتادنِ شبکه‌های کامپیوتری و ... در شرایط فوریت و اضطرار می‌باشد (Cybersecurity Malaysia, ۲۰۱۹).

قانون‌گذاری در ارتباط با فضای سایبری در مالزی

مقررات‌گذاری و قانون‌گذاری مقوله مهمی در ایجاد امنیت، اطمینان و اعتماد در ارتباط با هرگونه سیاست‌گذاری، برنامه‌ریزی و اجرا در ارتباط با حوزه "سایبری" است. هدف اصلی قانون‌گذاری در حوزه سایبری در کشور مالزی حمایت، تقویت و امنیت هشت حوزه کلیدی مرتبط با زیرساخت اطلاعات ملی این کشور است. براساس شواهد موجود، کشور مالزی متناسب

---

[۱] Cybercrime and Multimedia Investigation Branch

[۲] Special Cyber Court

[۳] Malaysia Computer Emergency Response Team (MyCERT)

با تغییر و تحولات سریعی که در حوزه آی.تی و فضای سایبر روی می‌دهد، قانون‌گذاری مناسب و بدنه قانون‌گذاری کافی برای مواجهه با هرگونه تغییر یا تهدید از این ناحیه را داشته است. برخی از مهم‌ترین قوانینی که مستقیماً و یا به صورت غیرمستقیم مربوط به حوزه سایبری می‌باشند، به شرح ذیل است:

جدول ۱: قوانین مرتبط با فضای سایبری در کشور مالزی

قوانینی که غیرمستقیم مربوط به حوزه سایبر است			قوانینی که مستقیم مربوط به حوزه سایبر است	
۱	Copyright Act 1987		۱	Communication & Multimedia Act 1998
۲	Sedition Act 1948		۲	Optical Disk Act 2000
۳	Panel Cod2015		۳	Computer Crime Act 1997
۴	Defamation Act 1957		۴	Digital Signature Act 1997
۵	Evidence Act 114A		۵	Telemedicine act 1997
			۶	Electronic Commerce act 2006
			۷	Electronic Government Activities Act 2007
			۸	Personal Data Protection Act 2010
			۹	Anti-Fake News Act 2018

نگاهی به تصویب و لغو قانون "ضد-اخبار جعلی" (۲۰۱۸) در مالزی

یکی از متأخرترین و جنجالی‌ترین قوانین مربوط به فضای سایبری در کشور مالزی، قانون "ضد-اخبار جعلی" بود که در اوایل سال ۲۰۱۸ و پس از مباحثه‌های فراوان در پارلمان این کشور به تصویب رسید. براساس این قانون "هرگونه خبر، اطلاعات، داده‌ها و گزارش‌هایی که کلاً یا جزئاً خلاف واقع است، خواه به شکل سرمقاله، ضبط صوتی یا تصویری یا به هر صورت دیگر که قابلیت اِلقاء کلمات یا افکار را داشته باشد"، خبر جعلی محسوب می‌شد. نکته جالب در ارتباط با این قانون، دامنه شمول آن بود که فراتر از مرزهای شهروندی و جغرافیایی این کشور را نیز در بر می‌گرفت. براساس این قانون، مادامی که "خبر جعلی" مربوط به کشور مالزی باشد، تمامی افراد اعم از شهروندان مالزیایی و یا اتباع غیرمالزیایی از هر کشور و همچنین در هر مکانی (اعم

از داخل و یا خارج از این کشور) مشمول این قانون می‌شدند و در صورت ارتکاب جرم، دولت مالزی موظف به پیگیری و برخورد با آن می‌شد.

بر اساس این قانون برای هرگونه تولید و هم‌رسانی آن چه که بر اساس این قانون، "خبر جعلی" یا "فیک نیوز" خوانده می‌شود، مجازات سنگینی در نظر گرفته شده بود که پرداخت جریمه ۵۰۰ هزار رینگیت (معادل ۱۳۰ هزار دلار) یا مجازات حبس ۶ سال و یا هر دو می‌توانست در انتظار فرد خاطی باشد. همچنین پس از محکومیت فرد خاطی و ناشر خبر جعلی، در صورت استمرار جرم، فرد خاطی می‌توانست روزانه به پرداخت ۳۰۰۰ رینگیت جریمه شود (Anti-Fake News Act 2018).

طرح این قانون و تصویب آن از همان ابتدا با مخالفت‌های جدی هم از سوی مخالفان داخلی دولت و هم از سوی نهادها و سازمان‌های بین‌المللی مواجه شد. به خصوص همزمان بودن طرح این قانون با چهاردهمین انتخابات سراسری در مالزی باعث شده بود تا مخالفان دولت و نیز سازمان‌های حقوق بشری از آن به عنوان ابزاری برای سرکوب آزادی بیان، تشویق روزنامه‌نگاران به خودسانسوری و در نهایت ایجاد فضای خفقان در کشور مالزی یاد کنند. این قانون اگرچه در نهایت تصویب و اجرایی شد، اما به دلیل تغییر دولت دوام چندانی نیافت.

البته چهاردمین دوره انتخابات پارلمانی در کشور مالزی مجالی برای تداوم این قانون جنجالی نداد. نتایج این انتخابات که به حاکمیت ۶۰ ساله حزب حاکم این کشور پایان داد، منجر به روی کار آمدنِ ائتلافی از احزاب اپوزیسیون شد که از ابتدا و براساس معیارهای حقوق بشری مخالف طرح و تصویب این قانون در پارلمان قبلی بودند. لذا، پس از آغاز به کار پارلمان چهاردهم و نیز روی کار آمدنِ دولت جدید به رهبری ماهاتیر محمد، یکی از اولین اقدامات این پارلمان لغو قانون "ضد اخبار جعلی" بود که با استقبال افکار عمومی و نیز نهادها و سازمان جهانی مواجه شد. این قانون در نهایت در آگوست سال ۲۰۱۸، تنها در حدود کمتر از ۶ ماه از زمان تصویب آن، لغو شد. هرچند اخیراً و به دنبال مواجهه جدید این کشور با سیل اخبار جعلی در فضای شبکه‌های اجتماعی، فرخوان‌های تازه ای مبنی بر تصویب مجدد قانون "ضد اخبار جعلی" همراه با جرح و تعدیل شنیده می شود.

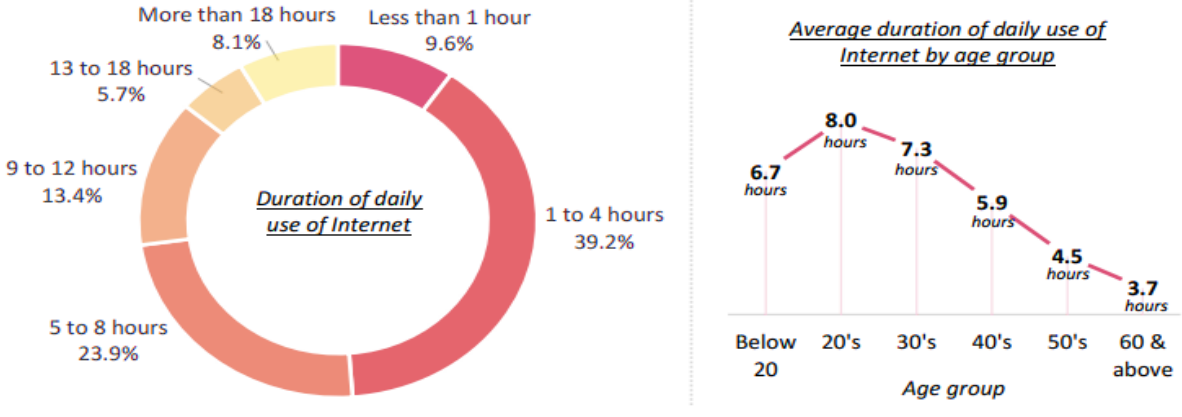
نظارت و فیلترینگ در فضای مجازی

مالزی یک کشور چند قومی، چند نژادی و چند مذهبی است. ضرورت ایجاد هارمونی و همزیستی مسالمت‌آمیز بین اقوام، نژادها و پیروان ادیان مختلف برای حفظ وجهه و پرستیژ این کشور به‌عنوان یک کشور اسلامی درحال‌توسعه و صلح‌طلب ایجاب می‌کند تا اینترنت و فضای سایبری نیز همانند سایر فناوری‌های ارتباطی و اطلاعاتی از مکانیسم‌های خاص نظارتی و کنترل برخوردار باشند.

در حال حاضر، کمیسیون ارتباطات و مولتی‌مدیای مالزی[۱] مسئول و متولی رصد و نظارت بر رسانه‌های این کشور، ازجمله اینترنت و فضای مجازی است و این کمیسیون از مکانیسم‌های قانونی و ابداعی مختلفی برای کنترل اینترنت و شبکه‌های اجتماعی استفاده می‌کند.

بر اساس گزارش کمیسیون ارتباطات و مولتی‌مدیای مالزی، ۸۷/۴ درصد مردم مالزی در سال ۲۰۱۸ به اینترنت و شبکه‌های اجتماعی دسترسی داشته‌اند که ۹۱ درصد آن از طریق تلفن هوشمند بوده است.

شکل ۰۱: میزان ساعات استفاده از اینترنت به تفکیک گروه‌های سنی در مالزی



منبع: پیمایش ملی اینترنت در سال ۲۰۱۸

[۱] Malaysian Communications and Multimedia Commission

در کشور مالزی، فیس‌بوک و واتس‌آپ محبوب‌ترین شبکه‌های اجتماعی محسوب می‌شوند. ۹۶/۵ درصد کاربران اینترنت در مالزی، صرفاً از شبکه‌های اجتماعی برای برقراری ارتباط با خانواده، دوستان و همکاران خود استفاده می‌کنند. ضمن آنکه که "محتوای آموزشی"، "محتوای سرگرم‌کننده و شایعات"، "اخبار"، "اطلاعات عمومی و اطلاعیه‌ها"، "تبلیغات تجاری و تخفیفات تجاری" و "موضوعات سیاسی" به ترتیب بیشترین اطلاعاتی است که از طریق شبکه‌های اجتماعی در بین کاربران ردوبدل می‌شود (The Internet User, 2018).

شکل ۲: توزیع استفاده از شبکه‌های اجتماعی در مالزی

منبع: پیمایش ملی اینترنت در سال ۲۰۱۸

"فیلترینگ" و "حذف محتوا" دو مکانیسم اصلی کمیسیون ارتباطات و مولتی‌مدیای مالزی برای اطمینان از سلامت و صیانت از فضای مجازی در این کشور است. هرچند اِعمال این دو مکانیسم بیشتر از طریق تعمیم قوانین فعلی و جاری مرتبط با رسانه‌ها (شامل ۱-قانون اسرار

رسمی[1] ۲-قانون فتنه[2] ۳-قانون مطبوعات چاپی و انتشار[3] ۴-قانون پخش[4] ۵- قانون امنیت ملی[5]۶- قانون سانسور فیلم[6] به اینترنت و شبکه‌های اجتماعی در فضای مجازی صورت می‌گیرد.

فیلترینگ: بر اساس دستورالعمل کمیسیون ارتباطات و مولتی‌مدیای مالزی، سایت‌های اینترنتی غیراخلاقی به‌خصوص سایت‌های پورنوگرافی ممنوع بوده و فیلتر می‌باشند. بااین‌وجود، قوانین فوق‌الذکر (به‌خصوص قانون فتنه، قانون اسرار رسمی، قانون امنیت ملی و ...)، دستاویز خوبی نیز در اختیار این کمیسیون قرار داده تا بر اساس آن، سایت‌های اینترنتی که توسط این کمیسیون "نامناسب" تشخیص داده شوند، نیز مورد فیلتر واقع شوند. این قوانین، همان‌طور که در ارتباط با سایر رسانه‌های چاپی و پخش مصداق می‌یابد، اجازه می‌دهد افراد به‌عنوان "مالکان" شبکه‌های اجتماعی یا وب‌سایت‌ها و یا افراد به‌عنوان "عاملان پخش" یا "عاملان انتشار" مطالبی که ناقض قوانین فوق باشند، تحت تعقیب قانون قرارگرفته و مطابق جرائم صورت گرفته و بر اساس مجازات تعیین‌شده، محکوم شوند.

صعوداح وک و شحفیذان محمد در ارزیابی خود از وضعیت اینترنت در این کشور خاطرنشان ساختند که این کمیسیون در سال ۲۰۱۴، بیش از ۶ هزار وب‌سایت را فیلتر کرده که ازجمله شامل وب‌سایت‌های سیاسی، خبری، اجتماعی و فرهنگی نیز بوده است. اِعمال سفت و سخت قوانین فعلی و تعمیم بیش‌ازحد آن به اینترنت و شبکه‌های اجتماعی بیش از هر چیزی باعث ایجاد "خودسانسوری" در مالزی شده است (Saodah Wok and Shafizan Mohamed, 2017).

حذف محتوا: دومین مکانیسم پُرکاربرد در ارتباط با فضای مجازی و شبکه‌های اجتماعی، صدور "فرمان حذف محتوا" از سوی کمیسیون ارتباطات و مولتی‌مدیا است. به‌طور خاص، بر

---

[1] Official Secrets Act (OSA)
[2] Sedition Act
[3] Printing Press Act (1984)
[4] Broadcasting Act (1987)
[5] Internal Security Act (ISA)
[6] Film Censorship Act (2002)

اساس قانون اساسی مالزی، هرگونه انتشار مطالب و یا اخبار علیه "دین اسلام" (اهل سنت و جماعت) و "نظام پادشاهی" کشور مالزی جرم محسوب می‌شود. ازاین‌رو، مطالبی با مضمون ضدیت با "دین اسلام" و یا "ضد نظام حاکم" بر این کشور، در صدر نظام مانیتورینگ کمیسیون ارتباطات و مولتی‌مدیا قرار داشته و در صورت مشاهده هر یک از آن‌ها، فرمان "حذف محتوای" مربوطه صادر می‌شود. در سال‌های پس از ۲۰۱۳ که دولت این کشور در تلاطم سیاسی زیادی قرار داشت، بارها از این قوانین به‌صورت غیرشفاهی علیه مخالفان دولت استفاده شده است. همچنین در سال‌های اخیر (به‌خصوص سال‌های ۲۰۱۵ و ۲۰۱۶) موارد زیادی از درخواست این کمیسیون از فیس‌بوک، یوتیوب و حتی صاحبان وبلاگ‌های شخصی مبنی بر حذف برخی محتواها وجود داشته است (Ahmad, 2009).

همکاری بین‌المللی مالزی در حوزه سایبری

مالزی به عنوان یک عضو فعال جامعه بین‌الملل همواره تلاش داشته نقش مؤثری در زمینه‌های مختلف در عرصه منطقه‌ای و بین‌المللی داشته باشد. اصولاً مالزی همواره در ارتباط با همکاری‌های منطقه‌ای و بین‌المللی رویکردی باز و ایجابی داشته است. عرصه سایبری نیز از این امر مستثنی نیست. از ابتدای ظهور شبکه‌های اجتماعی و شکل‌گیری فضای سایبری، دولت مالزی همواره مشارکت جدی در زمینه همکاری‌های بین‌المللی به خصوص در چارچوب اتحادیه منطقه‌ای کشورهای جنوب شرق آسیا (آ.سه.آن)، کشورهای عضو سازمان کنفرانس اسلامی[۱] (OIC) و کشورهای مشترک المنافع[۲]داشته است. همچنین در سال‌های اخیر، مالزی در ارتباط با "فضای سایبری"، رویکرد همکاری دوجانبه، سه‌جانبه و چندجانبه به‌ویژه با شرکای استراتژیک خود اتخاذ کرده است که از جمله می‌توان به همکاری دوجانبه با کره جنوبی،[۳] همکاری سه‌جانبه

[۱] Organization of Islamic Cooperation (OIC)

[۲] Commonwealth

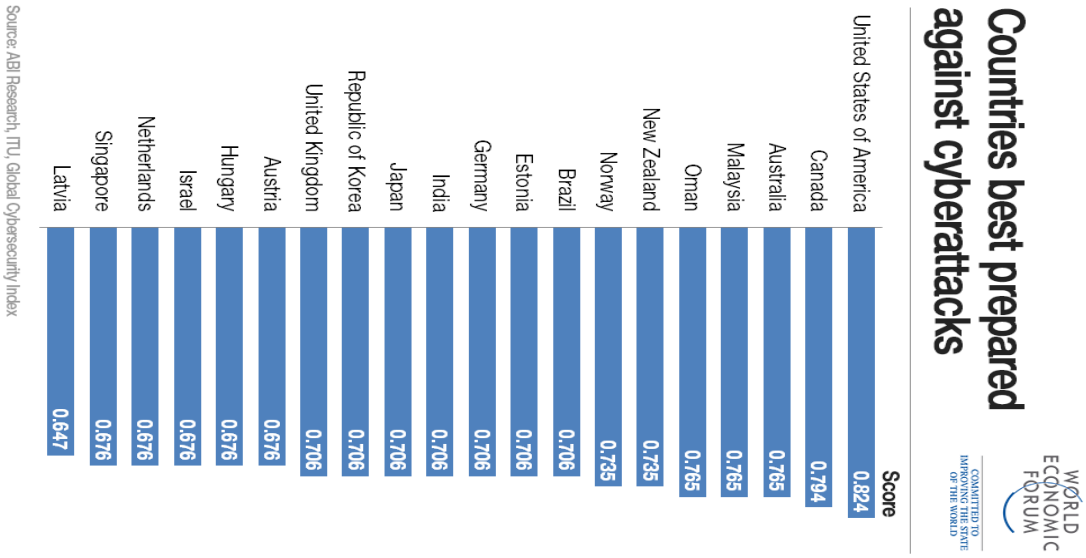
[۳] Memorandum of Agreement, Malaysia-Republic of Korea

با فیلیپین و اندونزی[۱] همکاری دوجانبه با استرالیا[۲] همکاری دوجانبه با هند[۳] و نیز همکاری با اتحادیه اروپایی[۴] اشاره کرد.

جایگاه جهانی مالزی به لحاظ حکمرانی سایبری

رویکرد باز و استقبال این کشور از همکاری‌های منطقه‌ای و بین‌المللی در حوزه فناوری‌های نوین ارتباطی و اطلاعات باعث تثبیت موقعیت این کشور در عرصه بین‌الملل در عمده حوزه‌ها، از جمله در زمینه فضای سایبری شده است. براساس ارزیابی‌هایی که توسط اتحادیه بین‌المللی ارتباطات راه دور در زمینه "آمادگی در حوزه حملات سایبری" صورت گرفته، مالزی در سال‌های اخیر همواره در بین ۲۰ کشور اول جهان قرار داشته است.

شکل ۱: جایگاه مالزی در بین ۲۰ کشور اول جهان از لحاظ حملات سایبری



ABI Research and ITU, Global cybersecurity Index

---

[۱] Trilateral Meeting on Security, Indonesia-Malaysia-Philippines

[۲] Memorandum of Understanding, Australia-Malaysia

[۳] Memorandum of Understanding, India-Malaysia

[۴] EU-Malaysia Partnership and Cooperation Agreement (PCA)

شکل ۰۲: رتبه‌بندی کشورها براساس شاخص امنیت سایبری

Country	GCI Score	Legal	Technical	Organizational	Capacity Building	Cooperation
Singapore	0.92	0.95	0.96	0.88	0.97	0.87
United States	0.91	1	0.96	0.92	1	0.73
Malaysia	0.89	0.87	0.96	0.77	1	0.87
Oman	0.87	0.98	0.82	0.85	0.95	0.75
Estonia	0.84	0.99	0.82	0.85	0.94	0.64
Mauritius	0.82	0.85	0.96	0.74	0.91	0.70
Australia	0.82	0.94	0.96	0.86	0.94	0.44
Georgia	0.81	0.91	0.77	0.82	0.90	0.70
France	0.81	0.94	0.96	0.60	1	0.61
Canada	0.81	0.94	0.93	0.71	0.82	0.70

(Global Cybersecurity 2017- International Telecommunication Union (ITU))

همچنین در ارزیابی سال ۲۰۱۷ این سازمان جهانی از وضعیت کشورها براساس پنج شاخص "قانونی"، "فنی"، "سازمانی"، "ظرفیت‌سازی" و "همکاری" داشته، مالزی با کسب نمره میانگین ۰,۸۹ رتبه دوم در آسیا و رتبه سوم جهانی پس از سنگاپور و آمریکا قرار گرفته است.[۱]

جمع‌بندی و نتیجه‌گیری

در ارزیابی نوع مواجهه مالزی با "فضای سایبر" می‌توان به وضوح غلبه رویکرد دفاعی و امنیتی را ملاحظه نمود. البته، این لزوماً منفی نیست. این کشور به‌رغم رسیدن به آستانه سال ۲۰۲۰، همچنان دوران گذار "تکنولوژیک" را تجربه می‌کند. وابستگی شدید حوزه‌های کلیدی "زیرساخت اطلاعاتی ملی" به فناوری‌های نوین اطلاعاتی و ارتباطی ایجاب می‌کند که رویکرد دفاعی و امنیتی با هدف اطمینان از کارایی و عملکرد این حوزه‌ها در مرکز ثقل هرگونه برنامه‌ریزی و سیاست‌گذاری قرارگیرد.

[۱] Global Cybersecurity Index (GCI),2017

وجه مثبت حکمرانی سایبری در مالزی، رویکرد ایجابی این کشور برای استفاده از ظرفیت‌ها و فرصت‌های فضای مجازی برای توسعه همه جانبه می‌باشد. این کشور حاکمیت "فناوری" در عصر سایبری را به رسمیت شناخته و به همین دلیل، در اغلب سیاست‌گذاری‌ها بر دستیابی به آخرین فناوری‌ها و نیز استفاده حداکثری از ظرفیت‌های فناوری و نوآوری تأکید کرده است. هرچند همین رویکرد ایجابی، آسیب‌ها و پیامدهای جدی نیز برای این کشور داشته است که از جمله آن، زیان ۱۲,۲ میلیارد دلاری اقتصادی ناشی از حملات سایبری به کشور مالزی می باشد. البته نباید از نظر دور داشت که رویکرد بی‌طرفانه و موضع نسبتاً خنثای این کشور در موضوعات و مسائل مهم بین‌المللی نیز تا حد زیادی به در"حاشیه امن" قرار گرفتن این کشور در چالش‌ها و تهدیدهای جدی بین‌المللی که "جنگ سایبری" و "جاسوسی سایبری" نیز از جمله آن‌ها محسوب می‌شود، کمک زیادی کرده است.

شاید بتوان گفت مهم‌ترین نقطه اتکای "حکمرانی سایبری" این کشور در عرصه داخلی "دفاعی و امنیتی" و در عرصه بین‌الملل نیز رویکرد همگرایانه با کشورهای خارجی به‌ویژه کشورهای پیشرفته همچون اتحادیه اروپا، آمریکا، استرالیا، کره جنوبی و ... در این عرصه است. مالزی هنوز فاصله زیادی به مرحله دستیابی به "اِشراف راهبردی" در حوزه سایبری برای پیشبرد اهداف توسعه‌ای خود دارد.

منابع و مآخذ

[1] Cyber policy Portal. Retrieved July 2019, from: Https://cyberpolicyportal.org/en/states/malaysia

[2] Cyber Security Malaysia Portal. Retrieved July 2019 from: https://www.cybersecurity.my/en/

[3] Global Cybersecurity Index (GCI) (2017), International Telecommunication Union (ITU).

[4] Ministry of Science, Technology and Innovation. "National R&D Roadmap for Self Reliance in Cyber Security Technologies." Unpublished.

[5] "National Cyber Security Policy: The Way Forward", Ministry of Science, Technology and Innovation, Malaysia, Federal Government Administrative Centre. July 2006.

[6] Mohd Shamir b Hashim (2011). Malaysia's National Cyber Security Policy: The Country's Cyber Defense Initiatives. Ministry of Science, Technology and Innovation, Malaysia.

[7] ISACA and the IT Governance Institute. ISACA Overview. Retrieved July 12, 2019. From http://www.isaca.org/About-ISACA /History/Pages /default.aspx.

[8] Anti-Fake News Act 2018. Laws of Malaysia.

حکمرانی فضای مجازی درکشورهای جهان: مالـزی

حـوزه فضـای مجـازی بـه انـدازه انقـلاب اسـلامی اهمیـت دارد. این فضا مثل یک رودخانه پر از آب و خروشان است که می آید و دائماً هم بر آب آن افزوده و خروشان‌تر می‌شود. اگر ما بر این رودخانه تدبیر کنیم و برنامه داشته باشیم، زه کشی کنیم و هدایت کنیم، این رودخانه را تا به سد بریزد، می‌شود فرصت. اگر رهایش کنیم و برنامه‌ای برای آن نداشته باشیم می‌شود یک تهدید.

۱۳۹۱/۷/۲

www.majazi.ir