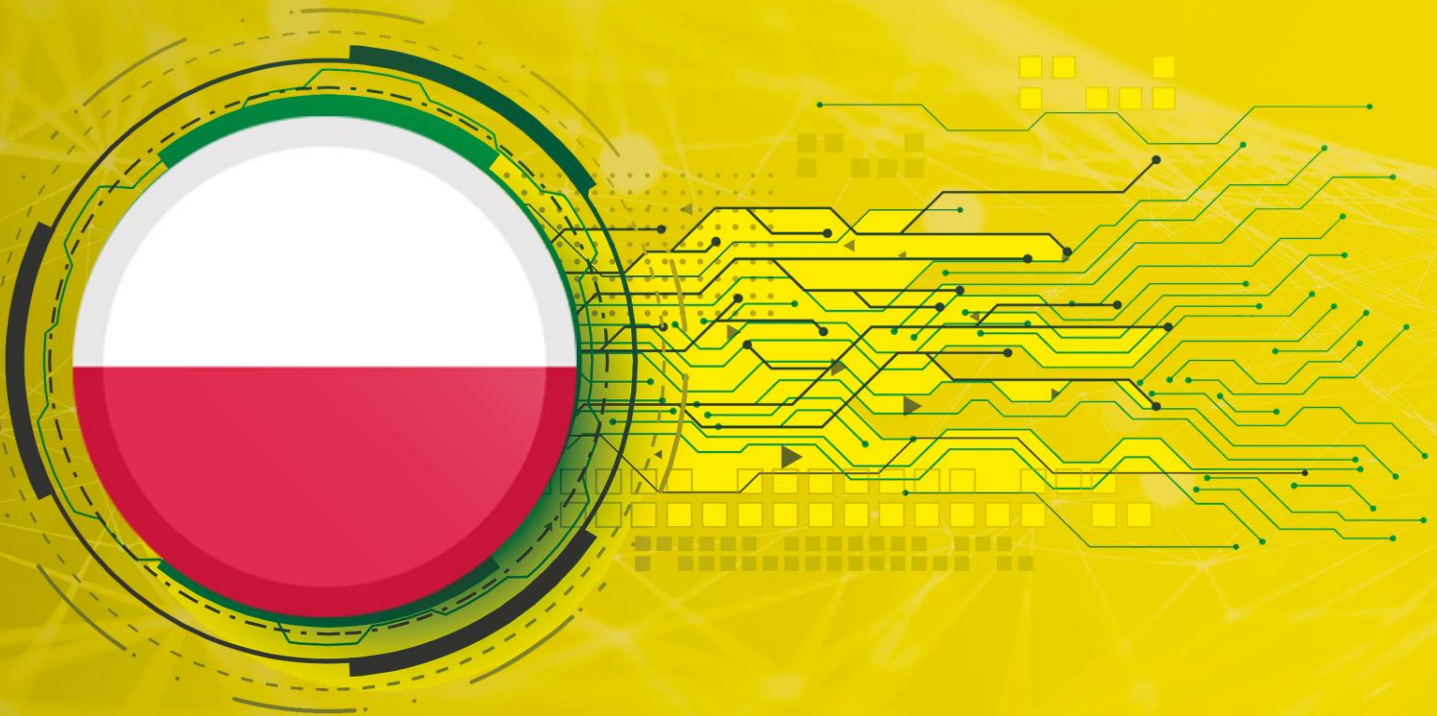


حکمرانی فضای مجازی در کشورهای جهان

لهستان





حکمرانی فضای مجازی در کشور لهستان

گزارش سریع (۱۰)

بهمن ماه ۱۳۹۸

تهیه شده در: پژوهشگاه مرکز ملی فضای مجازی - گروه مطالعات فرهنگی و اجتماعی

تهیه کننده: شیما وزوایی (کارشناس ارشد دانشگاه سن پترزبورگ)

ناظر علمی: امیررضا باقرپور شیرازی

نشانی: تهران، میدان آرژانتین، خیابان بیهقی، نبش خیابان ۱۶ غربی، پلاک ۲۰، کدپستی ۱۵۱۵۶۷۴۳۱۱

<http://www.majazi.ir>

شماره تماس: ۸۶۱۲۱۰۶۱

حقوق مادی و معنوی این اثر متعلق به مرکز ملی فضای مجازی است و استفاده از مطالب آن صرفاً با ذکر مأخذ بلامانع است.

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

هنگامی که از حکمرانی فضای مجازی سخن می‌گوییم، دست کم 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 اعمال 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 شکل دادن 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 لهستان خواهیم پرداخت.

واژگان کلیدی

حکمرانی فضای مجازی، لهستان، نظارت و فیلترینگ، وزارت امور دیجیتال لهستان، چارچوب ملی سیاست‌گذاری امنیت سایبری لهستان

فهرست مطالب

- ۱.....مقدمه
- ۲.....ساختار حکمرانی فضای مجازی در کشور لهستان
- ۳.....افتتاح دو اداره جدید در حوزه سایبری
- ۳.....نهادهای اصلی مسئول در حوزه فضای مجازی
- ۴.....قوانین مهم در حوزه فضای مجازی
- ۵.....رویکرد راهبردی در تدوین اسناد سیاستی
- ۵.....برنامه ها، رویه‌های اجرایی و اهداف تعیین شده
- ۶.....نظارت و فیلترینگ در فضای مجازی لهستان
- ۷.....رویکرد بین‌المللی
- ۸.....راهبرد امنیت سایبری لهستان
- ۸.....چارچوب ملی سیاست‌گذاری امنیت سایبری جمهوری لهستان ۲۰۱۷-۲۰۲۲
- ۱۰.....ساختار کلی و خروجی‌های سند چارچوب ملی
- ۱۱.....سناریوی حکمرانی فضای مجازی لهستان
- ۱۲.....منابع و مآخذ

مقدمه

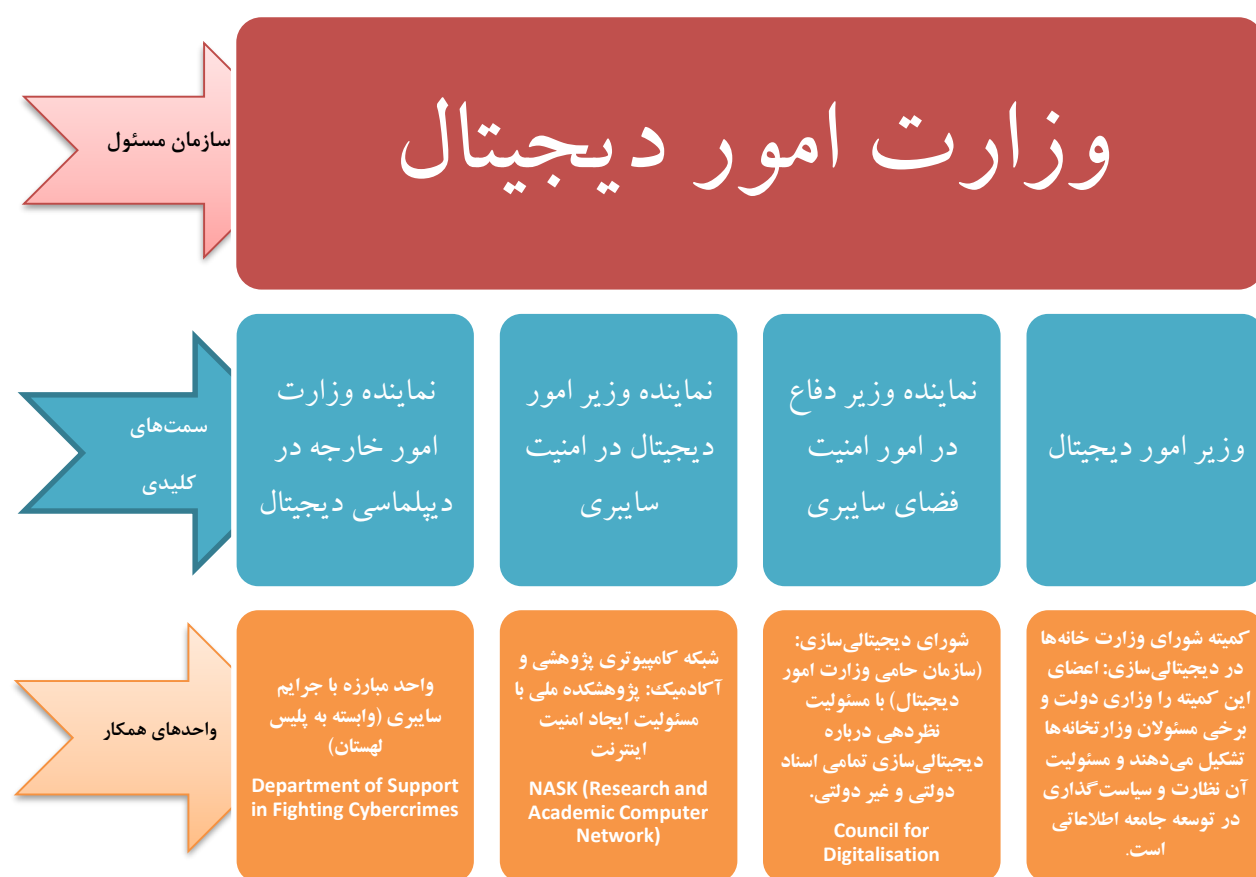
جمهوری لهستان کشوری با مساحت ۳۱۲ هزار کیلومتر مربع واقع در اروپای مرکزی و شرقی است. این کشور با جمعیت ۳۷,۵ میلیون نفر ششمین کشور پُرجمعیت اتحادیه اروپا است. پایتخت آن ورشو بوده و از جمله شهرهای مهم و بزرگ آن می‌توان به کراکوف، پوزنان و دانسک نام برد. همسایه‌های این کشور لیتوانی، استان کلینینگراد روسیه، بلاروس، اوکراین، اسلواکی، جمهوری چک و آلمان هستند. کشور لهستان از لحاظ امنیتی واحدی مستقل بوده و منافع امنیتی‌اش را بر اساس منافع ملی و اهداف راهبردی خود تعریف می‌کند. این استقلال و اهمیت و تأکید بر آن نتیجه بسترها و تجربه‌های تاریخی، شرایط و ساختارهای سیاسی و اجتماعی، و همین‌طور توانایی‌های دولت در برقراری امنیت ملی است.

در قرن بیست و یکم و عصر اطلاعات و فناوری‌های ارتباطاتی، دسترسی و امنیت اطلاعات و خدمات مربوط به آن از جمله ستون‌های اصلی امنیت ملی یک کشور به شمار می‌روند. در جمهوری لهستان نیز توجه ویژه به امنیت سایبری از این مهم مستثنی نبوده و همواره در اولویت دولت این کشور قرار داشته است. شاید رسیدن به استقلال سایبری (و در نتیجه استقلال ملی)، محافظت از آن، و در عین حال راضی نگه‌داشتن متحدان، شرکا، و نهادهای بین‌المللی ذی‌نفع و درگیر در ارتباط سیاسی با لهستان مهم‌ترین هدف و چالش این کشور در سیاست‌گذاری سایبری باشد. شایان ذکر است که سیاست‌گذاری اطلاعاتی و ارتباطاتی و دسترسی آزاد به اطلاعات برای شهروندان، نهادهای اجتماعی، اقتصادی، سیاسی و رسانه‌ای، و البته دولت لهستان همواره مورد انتقاد نهادهای مدنی و بین‌المللی بوده و برای بهبود آن از شیوه‌های تدافعی استفاده شده است. درک این وضعیت نیازمند کاوشی عمیق‌تر در چگونگی و چیرستی سیاست‌گذاری امنیت سایبری در این کشور و نحوه مدیریت تعهدات بین‌المللی به چارچوب‌های امنیت سایبری در اروپای شرقی و اتحادیه اروپا است. تشریح سیاست‌گذاری امنیت سایبری در جمهوری لهستان موضوع اصلی این گزارش است.

ساختار حکمرانی فضای مجازی در کشور لهستان

هدف از حکمرانی سایبری در لهستان توسعه زیرساخت‌های دسترسی به همگانی به اینترنت، حمایت از ایجاد محتواهای دیجیتال و خدمات الکترونیک در دولت و بخش خصوصی، ترویج آگاهی و سواد دیجیتال در میان شهروندان و ایجاد امنیت اطلاعات و ارتباطات در این کشور است. (UNIDIR, 2018)

شکل ۱: ساختار حکمرانی فضای مجازی لهستان



افتتاح دو اداره جدید در حوزه سایبری

از جمله نتایج حاصل از سند چارچوب ملی تشخیص نیاز و تبیین چگونگی بودجه‌بندی و طراحی دو واحد جدید و کلیدی در حوزه سایبری بود. این دو اداره عبارتند از:

اداره فضای سایبری دفتر نخست‌وزیر

وظیفه این اداره ارائه تحلیل، نظارت و ارزیابی بر انواع فعالیت‌های سایبری در سطح ملی و مهارت‌های سایبری بخش عمومی و بخش خصوصی و همکاری‌های بین‌بخشی است.

واحد نیروی فضای سایبری

وظیفه این واحد که در وزارت دفاع جمهوری لهستان با بودجه ۴۶۵ میلیون یورویی (UNIDIR, 2018) در حال احداث است، عملیات‌های نظامی و دفاعی در فضای سایبری است.

نهادهای اصلی مسئول در حوزه فضای مجازی

چشم‌انداز ۲۰۲۲ جمهوری لهستان برای تبدیل شدن به کشوری پیشرو در حوزه اطلاعات و تبدیل جامعه لهستان به جامعه تاب‌آور در برابر تهدیدهای داخلی و بین‌المللی سایبری از طریق تمرکز بر اقتصاد دیجیتال، امنیت دیجیتال و توسعه هم‌زمان داخلی و بین‌المللی فضای مجازی در این کشور و با همکاری چندین سازمان برجسته و عالی‌رتبه محقق خواهد شد. (National Framework of Cybersecurity, 2017)

جدول ۰۱: نهادها/سازمان‌های مسئول در سیاست‌گذاری سایبری و وظیفه اصلی آن‌ها

| ردیف | نهاد مسئول | وظیفه سازمان |
|------|------------------------|--|
| ۱ | اداره امنیت ملی BBN | تهیه دکترین امنیت سایبری، نقشه‌برداری دیجیتال از همه نهادهای دولتی، سازمان‌ها، نیروهای نظامی، بخش خصوصی و سازمان‌های مردم‌نهاد |
| ۲ | وزارت امور دیجیتال | وزارت امور دیجیتال که تا قبل از سال ۲۰۱۳ وزارت امور همگانی و دیجیتالی‌سازی نام داشت وظیفه راهبری تأمین امنیت سایبری در تمامی سطوح و تهیه چارچوبی قانونی و سازمانی برای آن را بر عهده دارد. |

| | | |
|---|------------------------------------|---|
| تأمین امنیت دولت در برابر تهدیدهای سایبری | آژانس امنیت داخلی ^۱ ABW | ۳ |
| تبیین راهبردهای دفاعی سایبری، تشخیص تهدیدها و حمله‌های سایبری | وزارت دفاع | ۴ |

قوانین مهم در حوزه فضای مجازی

هرچند قانون‌گذاری و اصلاح و بازبینی قانون‌های قدیمی‌تر در حوزه سایبری نقش مهم و اساسی در ایجاد احساس امنیت، رعایت حقوق شهروندان و ایجاد اعتماد بین دولت و بخش خصوصی است، اما کشور لهستان در این زمینه پیشرو نبوده است. در ادامه به سه قانون مهم در حوزه امنیت سایبری در جمهوری لهستان پرداخته شده است (آدامسکس،^۲ ۲۰۱۵).

جدول ۰۱: قوانین تصویب‌شده در حوزه امنیت سایبری در جمهوری لهستان

| موضوع | نام قانون | سال تصویب | ردیف |
|--|--|-----------|------|
| وزارت امور دیجیتال متعهد می‌شود به: ۱- اجرای کامل قوانین کمیسیون اروپا در حوزه امنیت سایبری، ۲- ایجاد نظام ملی امنیت سایبری در لهستان، ۳- ایجاد واحدی ارتباطی در وزارت امور دیجیتال برای تبادل اطلاعات با حداقل دو کشور عضو اتحادیه اروپا در صورت وقوع حوادث و حمله‌های جدی سایبری | قانون نظام ملی امنیت سایبری ^۳ | ۲۰۱۸ | ۱ |
| شرکت‌های مخابراتی متعهد می‌شوند که در صورت وقوع حوادث و حمله‌های سایبری مرکز ملی مخابرات را مطلع کنند. | قانون مخابرات ^۴ | ۲۰۱۳ | ۲ |
| به رسمیت شناختن جرائم سایبری از قبیل هک کردن، تقلب، دزدی اطلاعاتی و ... | قانون مجازات ^۵ | ۱۹۹۷ | ۳ |

^۱ Internal Security Agency

^۲ Adamski

^۳ Act on National Cybersecurity System (Krajowego Systemu Cyberbezpieczeństwa)

^۴ The Telecommunications Act (Dz.U. 2013 poz. 386)

^۵ Penal Code (No. 88, item 553, as amended)

رویکرد راهبردی در تدوین اسناد سیاستی

دولت جمهوری لهستان رویکردی راهبردی را به سیاست‌گذاری سایبری اتخاذ کرده است و بر تأمین امنیت تمامی اجزای فضای سایبری با راهبردهای جداگانه تأکید دارد. به همین دلیل برای تهیه سند چارچوب ملی از رویکردی بین-وزارت‌خانه‌ای استفاده شده است (National Framework of Cybersecurity, 2017).

شکل ۱: رویکرد بین‌وزارت‌خانه‌ای دولت لهستان برای تهیه چارچوب ملی سیاست‌گذاری



برنامه‌ها، رویه‌های اجرایی و اهداف تعیین شده

همان‌طور که گفته شد توسعه اجتماعی و اقتصادی هرچه بیشتر به دسترسی سریع و امن به اطلاعات و استفاده از فناوری اطلاعات در مدیریت، تولید و خدمات عمومی وابسته است. هرگونه اختلال در فضای سایبری، چه در سطح بین‌المللی و چه سطح ملی و محلی، بر فعالیت اقتصادی، احساس امنیت شهروندان و مولد بودن نهادهای دولتی و خصوصی و عمومی مؤثر است. امروزه امنیت ملی کشورها در گرو امنیت سایبری است و به همین دلیل جمهوری لهستان سیاست‌گذاری سایبری را در برنامه توسعه خود قرار داده است. چارچوب کلی سیاست‌گذاری سایبری در کشور

لهستان که وزارت امور دیجیتال این کشور مسئولیت تهیه آن را در سال ۲۰۱۷ میلادی بر عهده داشته بر سه اصل اساسی استوار است:

- احترام به حقوق و آزادی در فضای سایبری
- رویکردی جامع و یکپارچه به امنیت سایبری
- امنیت سایبری به عنوان عنصری مهمی از سیاست گذاری ملی

نظارت و فیلترینگ در فضای مجازی لهستان

موج تغییرات سیاسی پوپولیستی و گذار به جناح راست در اروپا باعث افزایش سیستم‌های نظارت بر گردش آزاد اطلاعات، سانسور محتواهای مشخص در فضای مجازی و در نتیجه کاهش آزادی‌های فردی در استفاده از اینترنت شده است. کشور لهستان نیز از این قاعده مستثنی نبوده است. در سال‌های اخیر قوانین محدودکننده‌ای برای استفاده اینترنت آزاد وضع شده است که بیشتر آن‌ها به عنوان «قوانین مبارزه با تروریسم سایبری» تصویب و به عموم معرفی شده‌اند. استفاده از شبکه‌های خصوصی یا Free Polish VPNs نه تنها در لهستان و بلکه در کشورهای دیگر دنیا هم معمول و باب طبع است. (Johnson, ۲۰۱۸)

بعضی از فعالین جامعه مدنی در حوزه سایبری معتقدند که قوانین نظارتی و ضد-تروریسم به گونه‌ای مبهم وضع شده‌اند که به دولت اجازه می‌دهد از آن‌ها برای محدود کردن محتواهای خاص و کنترل گردش محتوا و بایگانی هویت کاربران فضای سایبری استفاده کند. از جمله قوانین چالش برانگیز توانایی دولت در قطع کامل سیستم‌های مخابراتی و ارتباطاتی در هنگام بروز «تهدیدهای تروستی» است. همچنین در سال ۲۰۱۶ مکانیسمی برای فیلترینگ موضوعی محتواها و اپلیکیشن‌های خطرناک وضع شد که مجلس لهستان نیز با آن موافقت کرده و به تصویب رسانید. دولت همچنین به دنبال تصویب لایحه‌ای است که بر اساس آن شرکت‌های اینترنت خانگی موظف باشند اطلاعات افرادی که به محتواهای ممنوع دسترسی پیدا می‌کنند و

¹ Ministry of Digital Affairs

یا از وبسایت‌های فیلتر شده استفاده می‌کنند را در اختیار دولت قرار دهد. (Open ۲۰۱۶ Democracy). این تغییرات باعث نگرانی بخش خصوصی، سازمان‌های جامعه مدنی لهستانی و اروپایی شده و با توجه به رسانه‌ای شدن آن‌ها در سطح بین‌المللی به نظر می‌آید برای ارتباطات سیاسی همکاری‌های لهستان به شرکای اروپایی در دسرساز شود.

رویکرد بین‌المللی

در جمهوری لهستان سیاست‌گذاری سایبری و امنیت سایبری چالشی مهم برای تمامی واحدهایی است که با نحوی با اطلاعات و اینترنت سروکار دارند، از جمله: واحدهای تجاری، اقتصادی و خدمات فناوری‌های ارتباطاتی و اطلاعاتی، واحدهای عملیاتی، بخش‌های عمومی و تخصصی و البته نهادهای دولتی. به همین دلیل و نیز ساختار حکمرانی لهستان، موقعیت جغرافیایی آن و جغرافیای سیاسی اروپا مهم است که لهستان در همکاری نزدیک بین‌المللی با سازمان‌هایی از قبیل اتحادیه اروپا، ناتو، سازمان ملل و OSCE^۱ سازمان امنیت و همکاری در اروپا باشد. عضویت جمهوری لهستان در سازمان‌های منطقه‌ای و بین‌المللی از دو جهت در حوزه سیاست‌گذاری سایبری مهم است.

- از جهت تعهداتی که این کشور باید در حوزه سیاست‌گذاری، قانون‌گذاری و اجرای قانون داشته باشد.
- از جهت دریافت کمک و حمایت‌های دیجیتالی، مالی و امنیتی در حوزه سایبری

^۱ Organization for Security and Co-operation in Europe

راهبرد امنیت سایبری لهستان

چارچوب ملی سیاست گذاری امنیت سایبری جمهوری لهستان ۲۰۱۷-۲۰۲۲

مهم‌ترین و جدیدترین سند دولتی که تا به حال در حوزه سیاست گذاری سایبری در لهستان تدوین شده است «چارچوب ملی سیاست گذاری امنیت سایبری جمهوری لهستان ۲۰۱۷-۲۰۲۲» نام دارد. این سند راهبردی فرآیندی عملی دولت لهستان برای بالابردن امنیت سایبری در این کشور را تبیین و توضیح می‌دهد. سند مهم قبلی که تا پیش از سال ۲۰۱۷ نقشه راه دولت لهستان در حوزه سیاست سایبری بود «سیاست گذاری برای حفاظت از فضای سایبری در جمهوری لهستان»^۲ نام داشت. این سند در سال ۲۰۱۳ تنظیم و در سال ۲۰۱۴ تصویب شده بود. هردو این اسناد برای عموم قابل دسترس بوده و به زبان‌های لهستانی و انگلیسی وجود دارند. در این سند چهار هدف‌گیری عمده برای برقراری امنیت سایبری در لهستان مشخص شده است. این هدف‌گیری‌ها به شرح زیر هستند:

هدف اول - افزایش ظرفیت ملی برنامه‌ریزی عملی برای پیشگیری، تشخیص و کمینه کردن حوادثی که امنیت فناوری‌های اطلاعاتی و ارتباطاتی که به اداره دولت مربوط می‌شوند را به خطر می‌اندازند. این هدف شامل موارد ذیل می‌شود:

الف) تصویب قوانین لازم که پاسخگوی نیازهای و چالش‌های امنیت سایبری در لهستان باشند.
ب) بهبود ساختار نظام امنیت ملی سایبری، از جمله سازمان‌های جامعه مدنی و بخش خصوصی.

پ) افزایش تأثیر همکاری با واحدهای مختلفی که به نوعی در امنیت سایبری لهستان نقش دارند

ت) افزایش و تقویت امنیت خدمات دیجیتال و زیرساخت‌های حیاتی دولت

¹ National Framework of Cybersecurity Policy of the Republic of Poland for 2017-2022

² Policy for the Protection of Cyberspace of the Republic of Poland

ث) توسعه و اجرای استانداردهای عملکرد مثبت در حوزه امنیت شبکه و نظام‌های اطلاعاتی
 ج) توسعه و اجرای مدیریت ریسک در سطح ملی
 چ) کسب اطمینان از وجود و ساختن سیستمی برای هشداردهی در صورت حمله و تهدیدهای
 سایبری در سطح ملی و بین‌المللی

هدف دوم – تقویت ظرفیت مبارزه با تهدیدهای سایبری. این هدف شامل موارد ذیل می‌شود:
 الف) تقویت ظرفیت مبارزه با جرائم سایبری از جمله جاسوسی و تروریسم
 ب) ظرفیت‌سازی برای توانایی اقدام کامل نظامی در حوزه سایبری
 پ) ظرفیت‌سازی برای توانایی تحلیل مسائل امنیتی در سطح ملی^۱
 ت) ایجاد سیستم ارتباطاتی امن در حوزه امنیت ملی. (ایجاد کانال‌های ارتباطی امن با ناتو،
 اتحادیه اروپا، امنیت مخابرات، پست‌های الکترونیک و ...)
 ث) انجام مانورها و آزمایش‌های امنیتی سایبری

هدف سوم – افزایش پتانسیل و توانایی ملی در حوزه امنیت فضای سایبری. این هدف شامل
 موارد ذیل می‌شود:

الف) توسعه منابع صنعتی و تکنیکی با اهداف ارتقای امنیت سایبری (از جمله توسعه سکوه‌های
 مجازی برای برقراری امنیت سایبری کسب‌وکارهای خرد، نوپا و بزرگ)
 ب) توسعه مکانیسم‌های همکاری‌های سایبری در حوزه عمومی و بخش خصوصی
 پ) تحقیق و توسعه در حوزه امنیت اطلاعاتی، ارتباطاتی و امنیت فضای سایبری (نیازمند
 گسترش همکاری‌های دانشگاهی)
 ت) ارتقا توانایی افراد شاغل در حوزه امنیت سایبری
 ث) ایجاد شرایطی برای استفاده امن و مطمئن شهروندان از فضای مجازی

¹ Cyberspace was recognised by NATO as another domain of law enforcement operations at the NATO Summit in Warsaw in 2016.

هدف چهارم – ایجاد موقعیت مستحکم بین‌المللی برای لهستان در حوزه امنیت سایبری.

این هدف شامل موارد ذیل می‌شود:

الف) همکاری بین‌المللی مداوم در سطح سیاسی و راهبردی در حوزه امنیت سایبری و

بازارهای دیجیتال

ب) همکاری بین‌المللی مداوم در سطح عملی و تکنیکی

سند چارچوب ملی توسط گروهی از نمایندگان وزارت امور دیجیتال، وزارت دفاع، وزارت کشور و همچنین نمایندگانی از آژانس امنیتی داخلی، مرکز دولتی امنیت و اداره امنیت ملی تهیه شده است. شایان ذکر است که پیش‌شرط اجرا و موفقیت سند چارچوب ملی، اقدام دولت لهستان برای افزایش دسترسی همگانی به اینترنت و اطلاعات و همین‌طور پایان و اصلاح پروژه‌های دیجیتالی‌سازی حکمرانی در این کشور است. مسئولیت حکمرانی دیجیتال بر عهده وزارت امور دیجیتال جمهوری لهستان است.

ساختار کلی و خروجی‌های سند چارچوب ملی

به‌طور کلی ساختار و نتایج حاصل از تدوین سند چارچوب ملی سیاست‌گذاری برای امنیت

سایبری در جمهوری لهستان را می‌توان در ۸ بخش خلاصه کرد. (UNIDIR, 2018)

جدول ۱: ساختار کلی و خروجی‌های سند چارچوب ملی سیاست‌گذاری برای امنیت سایبری

| | |
|---|---|
| ۱ | تبیین و تشریح هدف‌گیری‌های لازم برای امنیت فناوری‌های اطلاعاتی و ارتباطاتی ICT |
| ۲ | تشخیص و تعیین تمامی عوامل و مسئولان درگیر در سیاست‌گذاری سایبری، از طراحی تا اجرا و نظارت |
| ۳ | تبیین ساختار مدیریتی لازم برای رسیدن به اهداف تعیین شده در سند چارچوب ملی |

¹ Internal Security Agency

² National Security Bureau (BBN)

| | |
|---|--|
| ۴ | مواجهه با تهدید، خطر و اتفاق ناگهانی در حوزه سایبری؛ اقدامات لازم برای پیشگیری، مواجهه با اتفاق و حمله سایبری، نحوه بازگرداندن شرایط به حالت اولیه. این بخش شامل تبیین نحوه همکاری دولت با بخش خصوصی نیز می‌شود. |
| ۵ | رویکرد لازم برای تخمین میزان ریسک در مسائل مختلف مربوط به سیاست‌گذاری سایبری |
| ۶ | آموزش، اطلاع‌رسانی و مهارت‌آموزی؛ همچنین برنامه‌های توسعه در حوزه سایبری و امنیت سایبری |
| ۷ | فعالیت‌های مربوط به پژوهش در حوزه سایبری |
| ۸ | هموارسازی مسیرهای لازم برای توسعه همکاری‌های بین‌المللی در حوزه امنیت سایبری |

سناریوی حکمرانی فضای مجازی لهستان

سناریوهای حکمرانی فضای مجازی کشور لهستان را می‌توان در قالب موارد زیر دسته بندی نمود:

- حرکت به سوی دیجیتالی سازی تمامی امور
- همسویی کامل با قوانین و ارزش های اتحادیه اروپایی
- در سال های اخیر، لهستان همسویی بسیار زیادی با سیاست‌های آمریکا، حتی در درون اتحادیه اروپایی از خود نشان داده است.

منابع و مآخذ

- [1] Agnija Tumkevič. (2016). Cybersecurity in Central Eastern Europe: From Identifying Risks to Countering Threats. ISSN 2335-2337, ISSN 2424-5488 (Online). Baltic Journal of Political Science. December 2016, No 5 DOI: <https://doi.org/10.15388/BJPS.2016.5.10337> Retrieved 15 July 2019
- [2] Andrzej Adamski. (2015). Cyber Legislation in Poland. Nicolaus Copernicus University, DOI: 10.13140/RG.2.1.1946.2249 available at https://www.researchgate.net/publication/279191115_CYBERCRIME_LEGISLATION_IN_POLAND Retrieved 15 July 2019
- [3] Bram Johnson. (2018). Internet Censorship and Surveillance in Poland. Available at <https://vpnalert.com/blog/poland-internet-censorship/> Retrieved 15 July 2019
- [4] European Agency for Cybersecurity, Polish National Cyber Security files, available at <https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/strategies/govermental-program-for-protection-of-cyberspace-for-the-years-2011-2016-2013> Retrieved 15 July 2019
- [5] Cyber Policy Portal, UNIDIR, Poland States, (2018). (PDF) available at <https://cyberpolicyportal.org/en/states/poland> Retrieved 15 July 2019
- [6] National Framework of Cybersecurity Policy of the Republic of Poland for 2017-2022
- [7] (PDF) Available at https://ccdcoe.org/uploads/2018/10/NCSO_Poland_2017.pdf Retrieved 15 July 2019
- [8] National Security Strategy of the Republic of Poland, (2014) PDF Warsaw, 2014
- [9] Poland Welcomes Internet filtering, 2017
- [10] <https://www.opendemocracy.net/en/poland-welcomes-internet-filtering/> Retrieved 15 July 2019
- [11] World Population Review. (2019). <http://worldpopulationreview.com/countries/poland-population/> Retrieved 15 July 2019

حکمرانی فضای مجازی در کشورهای جهان: لهستان

حوزه فضای مجازی به اندازه انقلاب اسلامی اهمیت دارد. این فضا مثل یک رودخانه پراز آب و خروشان است که می آید و دائماً هم بر آب آن افزوده و خروشان تر می شود. اگر ما بر این رودخانه تدبیر کنیم و برنامه داشته باشیم، زه کشی کنیم و هدایت کنیم، این رودخانه راتا به سد بریزد، می شود فرصت. اگر رهایش کنیم و برنامه ای برای آن نداشته باشیم می شود یک تهدید.

محمد مجاز

۱۳۹۱/۷/۲

