ضرورت‌ها و الزامات تدوین راهبرد سایبری کارآمد

قاسم ترابی*

مقدمه

کشورها برای مقابله با تهدیدات رو به گسترش سایبری و همچنین کسب فرصت‌های گسترده و جلوگیری از عقب‌ماندگی سایبری، نیازمند تدوین راهبرد سایبری جامع و کارآمدی مطابق با ماهیت خاص و پویای فضای سایبر هستند. بدین منظور تقریباً تمام کشورهای توسعه‌یافته سایبری طی چند سال گذشته حداقل یک یا چند راهبرد سایبری داشته‌اند. برای نمونه، ایالات‌متحده آمریکا به‌عنوان پیشگام‌ترین کشور دنیا در حوزه سایبری، در کنار سایر کشورهای عضو ناتو، دارای حداقل دو یا سه راهبرد سایبری هستند که تاکنون عملیاتی شده‌اند. بر اساس این ضرورت و به دلیل اهمیتی که فضای سایبر در بعد فرصت‌ها و تهدیدات دارد و نقش برجسته قدرت سایبری در جایگاه کشورها در سلسله‌مراتب قدرت جهانی، سؤال اساسی این است که در تدوین و تکامل راهبرد سایبری موفق، جامع و کارآمد باید به چه نکات، ضرورت‌ها و الزاماتی توجه شود. در پاسخ به این سؤال اساسی می‌توان گفت که با توجه به محتوای خاص فضای سایبر، تجربه سایر کشورها در تدوین راهبرد سایبری و عملکرد کشورهای عضو ناتو می‌توان به مواردی چون ضرورت توجه به ساختار سایبری، سرمایه‌گذاری و علم‌گرایی سایبری، حمایت گسترده از بخش خصوصی سایبری، داشتن

* دانشیار روابط بین‌الملل، واحد همدان، دانشگاه آزاد اسلامی، همدان، ایران

رویکرد جامع و ضرورت تدوین حقوق سایبری در داخل اشاره کرد. در ادامه به هرکدام از این موارد بیشتر پرداخته می‌شود.

۱. شناخت سایبری

اولین نکته مهم در ارتباط با تدوین راهبرد سایبری جامع و کارآمد که بتواند تأمین‌کننده امنیت سایبری باشد، موضوع فهم و شناخت جامع و دقیق نسبت به ضرورت و تدوین چنین سندی با توجه به خطرها و تهدیدهای فضای سایبری است. در این زمینه باید اشاره کرد که برخی از کشورها هنوز چندان نسبت به ضرورت داشتن راهبرد سایبری جامع و اصولاً میزان خطرها و تهدیدهای فضای سایبری حساس و نگران نیستند. برای نمونه، تجربه حملات سایبری روسیه علیه کشورهایی چون استونی، اوکراین و گرجستان نشان داد این کشورها تقریباً فاقد هرگونه آمادگی لازم در حوزه سایبری و اصولاً هرگونه سند، راهبرد یا سیاست روشنی در این زمینه هستند. این شرایط احتمالاً در مورد بسیاری از کشورهای جهان به‌ویژه در مناطقی همچون خاورمیانه که امنیت عمدتاً در سطح نظامی دیده می‌شود، نیز صادق است. این در شرایطی است که کشورهایی مانند آمریکا کم‌وبیش از دهه ۱۹۷۰ ضمن فهم چنین ضرورتی، دارای برنامه و سیاست‌های مشخصی در حوزه سایبر بوده‌اند. رژیم صهیونیستی نیز در دهه ۱۹۹۰ چنین ضرورتی را تشخیص داد و کارگروهی را برای درک فضای سایبر و ارائه راه‌کارهای امنیتی و اطلاعاتی تشکیل داد. این کارگروه پس از انجام کارهای تحقیقاتی گسترده، به سران این کشور ضرورت تدوین سند سایبری و ایجاد مراکز و مؤسساتی در زمینه جنگ و دفاع سایبری را توصیه کرد. رهبران رژیم صهیونیستی نیز نتایج این تحقیقات را جدی گرفتند و تلاش گسترده‌ای کردند تا پیشنهادات کارگروه‌ها را عملی کنند. در نتیجه در حال حاضر رژیم صهیونیستی دارای چند راهبرد سایبری مشخص، زیرساخت‌ها، مراکز و نیروهای حرفه‌ای در زمینه جنگ سایبری است. لازم به اشاره است که رژیم صهیونیستی در حال حاضر یکی از کشورهای پیشرو در زمینه امنیت سایبری است.

بر این اساس و با توجه به تجربه سایر کشورها می‌توان گفت که اولین قدم در حوزه تدوین راهبرد سایبری کارآمد یا اصلاح راهبرد سایبری موجود، فهم دقیق و جامع از اوضاع و

احوال فضای سایبر است؛ که ویژگی‌های اصلی آن عبارتند از ابهام، پیچیدگی، تغییر مداوم، گستردگی و در نتیجه سخت کنترل‌بودن. نکته مهم اینکه در صورتی‌که این فهم و ضرورت اولیه دقیق و واقع‌گرایانه نباشد، نه‌تنها کمکی به تدوین و اجرای سند راهبرد سایبری موفق نمی‌کند، بلکه عملاً می‌تواند سبب‌ساز مسائل، مشکلات و آسیب‌پذیری‌های عمده آینده باشد. برای نمونه، در حالی‌که بسیاری از کشورها در حوزه سایبری بر اقدامات تدافعی صرف که عمدتاً بر پایه سیاست واکنشی قرار دارد تأکید می‌کنند، تجربه چند سال گذشته نشان داده است که این سیاست‌ها تا چه میزان ناکارآمد هستند.

اما موضوع مهم‌تر این است که چگونه می‌توان به فهمی جامع و دقیق از فضای سایبر رسید؟ براساس تجربه سایر کشورها، فهم جامع و دقیق تنها زمانی حادث می‌شود که همکاری جدی بین دولت و به‌ویژه بخش‌های خصوصی و دانشگاه‌ها در اولویت قرار گیرد. واقعیت این است که موضوع امنیت سایبری و به شکل کلی، فضای سایبر به‌گونه‌ای است که دولت بدون همکاری بخش‌های خصوصی و به‌ویژه دانشگاه‌ها و مراکز علمی و پژوهشی نمی‌تواند شناخت جامع و دقیقی از آن به دست آورد. بر این اساس، همکاری بین بخش‌های مختلف دولت با چنین مراکزی و تشکیل کارگروه‌های حرفه‌ای و مشترک از رشته‌های مختلف مرتبط با موضوع، اولین گام در مسیر تدوین یک راهبردی سایبری کارآمد به‌حساب می‌آید.

۲. شکل‌دهی به ساختار سایبری کارآمد

در زمینه ایجاد ساختار کارآمد سایبری، آنچه بر اساس تجربه سایر کشورها می‌توان گفت، این است‌که در هر کشوری اول باید نهاد مسئول اصلی در مدیریت کلان فضای سایبر مشخص شود. تعیین نهاد یا مرکزی خاص در حوزه سایبری که از نظر قدرت بالاتر از تمام نهادی مسئول سایبری باشد، یکی از مهم‌ترین ضروریات در تدوین راهبرد سایبری موفق است. وجود چنین مرکز یا نهادی که عمدتاً نقش سیاست‌گذار، برنامه‌ریز، نظارت‌کننده و نقش رابط بین دولت و بخش خصوصی را دارد، باعث جلوگیری از موازی‌سازی، دوباره‌کاری، هدررفتن سرمایه‌ها و در مجموع سامان دادن به‌تمامی استعداد و توان کشور در ارتقاء امنیت سایبری

می‌شود. بر این اساس، در تعیین ساختار سایبری نکته اول ایجاد مرکز یا نهاد مسئول قوی و دارای اختیارات لازمی در حوزه سایبری است.

تقریباً در تمام کشورهای پیشرفته سایبری، این نهاد یا مرکز یا یکی از وزارتخانه‌ها زیر نظر شخص اول کشور است و یا مرکز یا نهادی مجزا که زیر نظر شخص اول اجرایی کشور فعالیت می‌کند. برای نمونه، در اسرائیل دفتر سایبری رژیم صهیونیستی[۱] این نقش را زیر نظر شخص نخست‌وزیر برعهده دارد. بعد از ایجاد چنین مرکزی، اولویت باید تشکیل مراکزی برای دفاع و تهاجم سایبری و ارتقا قدرت آن‌ها باشد. نکته مهمی که در این زمینه باید در نظر داشت، این است‌که در برخی از کشورها حوزه تهاجمی از دفاعی جداشده تا با ایجاد رقابت سالم عملاً توان تدافعی و تهاجمی کشور به شکل هم‌زمان ارتقاء پیدا کنند. البته در برخی از کشورها وظیفه دفاع و تهاجم سایبری به نیروی خاصی داده شده، اما در دل همان نیروی خاص دو تیم با عناوین خاص مثل گروه آبی یا قرمز ایجاد می‌شوند تا یکی وظیفه تهاجم و دیگری وظیفه دفاع را به عهده داشته باشد. نکته بعدی این‌که علاوه بر داشتن نیروی خاص دفاعی و تهاجمی در حوزه سایبری، هرکدام از نیروهای نظامی و دفاعی و همچنین اطلاعاتی و امنیتی باید نیروی سایبری خاص خود را داشته باشد؛ تا تهاجم و دفاع سایبری به شکل شبکه‌ای باشد. در ایالات‌متحده آمریکا، نیروی هوایی، دریایی، زمینی و وزارتخانه‌ها از جمله وزارت دفاع و وزارت امنیت سرزمینی، سازمان‌های اطلاعاتی و امنیتی از جمله «سیا» دارای نیروی سایبری خاص خود هستند. یا در اسرائیل علاوه بر یگان ۸۲۰۰ که در حوزه سایبری فعال است، هرکدام از نیروهای نظامی و دفاعی و اطلاعاتی دارای نیروی سایبری خاص خود هستند.

۳. علم‌گرایی سایبری

در حوزه سایبر، مهم‌ترین عامل قدرت ملی یک کشور و همچنین مهم‌ترین عامل امنیت سایبری، دانش سایبری است. به تعبیری دیگر، دانش سایبری عین قدرت است. به همین دلیل، سال‌هاست بین کشورها رقابت بسیار گسترده‌ای در حوزه دانش و قدرت سایبری وجود دارد؛

---

۱. Israel National Cyber Bureau (INCB)

چون آنان به‌خوبی می‌دانند که آنچه در آینده سلسله‌مراتب قدرت جهانی را شکل خواهد داد، قدرت سایبری برآمده از دانش سایبری است. در راستای این اهمیت، کشورهای پیشرفته سرمایه‌گذاری بسیار گسترده‌ای در حوزه سایبر کرده‌اند. برای نمونه، آمریکا به‌عنوان پیشرفته‌ترین کشور جهان، حوزه سایبری را یکی از اولویت‌های خود قرار داده است. همچنین، اسرائیل در راهبرد سایبری خود، اولویت اول را سرمایه‌گذاری گسترده در حوزه سایبری تا تبدیل‌شدن به قدرت سایبری جهان قرار داده است. بر این اساس، در راهبرد سایبری کارآمد باید بر تحقیق و تفحص سایبری تمرکز کرد و با سرمایه‌گذاری گسترده در تمامی حوزه‌ها و بخش‌هایی که می‌توانند به گسترش دانش سایبری کمک کنند، ظرفیت علمی سایبری کشور را گسترش داد.

در این راستا و بر اساس تجربه سایر کشورها سایبری می‌توان گفت سرمایه‌گذاری در حوزه دانش سایبری حداقل چندمحور مشخص دارد. در این زمینه، قدم اول، ارائه دروس مقدماتی سایبری در مدارس ابتدایی تا دبیرستان یا همان مقاطع قبل از دانشگاه است. هدف از این کار، آماده‌کردن نسل جدید برای آشنایی عمیق‌تر با فضای سایبر و در نهایت علاقه‌مندکردن آن‌ها و شناخت استعدادهای سایبری برای سرمایه‌گذاری و آینده‌سازی است. مرحله دوم، ایجاد رشته‌های سایبری در دانشگاه‌ها برای جذب استعدادهای سایبری و تبدیل آنها به نخبگانی است که در آینده می‌توانند تأمین‌کننده قدرت و امنیت سایبری کشور باشند. در این زمینه می‌توان به اسرائیل اشاره کرد. این رژیم با سرمایه‌گذاری گسترده و ارائه دروس سایبری از ابتدایی تا دانشگاه، استعدادها را شناسایی و با بورس آن‌ها در داخل یا خارج، در حال پرورش طیف گسترده‌ای از نخبگان سایبری است. همچنین، اسرائیل در سطح دانشگاهی، رشته‌های گسترده‌ای در حوزه سایبری دارد و با پیونددادن دانشگاه‌های خود با سایر کشورها به‌دنبال جذب اساتید و دانش سایبری دیگر کشورهاست. قدم دیگر در این زمینه، داشتن پژوهشکده‌های سایبری است که در آن اساتید، نخبگان و کارشناسان با حمایت دولت و بخش خصوصی، تحقیق و تفحص را در اولویت قرار دهند. نقش برجسته پژوهشکده‌ها و مراکز سایبری این است که به‌عنوان حلقه رابط بین دولت و بخش خصوصی، دانشگاه‌ها و بخش صنعت و حتی بین مردم و دولت عمل کرده و دانش سایبری را به قدرت عینی سایبری تبدیل

می‌کنند. پژوهشکده‌های سایبری همچنین می‌توانند به‌عنوان بازوی تحقیقاتی مراکز دولتی ایفای نقش کنند و نتایج تحقیقات خود را از طریق عالی‌ترین مراکز سایبری به شخص اول کشور گزارش کنند.

٤. حمایت از ایجاد و رشد صنعت سایبری

یکی از نشانگان پیشرفت در حوزه سایبری، داشتن صنعت سایبری پیشرفته، شرکت‌های سایبری موفق و کارآمد و بخش خصوصی است که توانمندی فراوانی در حفظ امنیت سایبری خود دارند. در واقع، یکی از نتایج سرمایه‌گذاری و علم‌گرایی سایبری، داشتن بخش خصوصی قوی سایبری است. پیشرفته‌ترین کشور جهان در این زمینه، آمریکا است که با اختلاف فراوان، ثروتمندترین، بزرگ‌ترین و کارآمدترین بخش خصوصی سایبری و شرکت‌های موفق سایبری را دارد. یکی دیگر از نشانگان قدرت کشورها در حوزه صنعت سایبری، توان شرکت‌ها و صنایع خصوصی در دفاع از امکانات و تأسیسات خودشان است. برای نمونه، در آمریکا، شرکت‌های خودروسازی، سرمایه‌گذاری فراوانی در حوزه سایبر کرده‌اند تا هم مانع اقدام سایر کشورها در جاسوسی صنعتی سایبری شوند و هم اینکه در مقابل حملات سایبری داخلی و خارجی امن باشند. به هرحال، در جنگ سایبری واقعی بین کشورها، بخش صنعت از اولین اهداف سایبری محسوب می‌شوند. با توجه به این شرایط، در تدوین راهبرد سایبری کارآمد، باید اولویت بالایی به بخش خصوصی قوی در حوزه سایبری داد. همچنین، باید برنامه‌ریزی گسترده‌ای کرد تا سایر بخش‌های صنعتی کشور که لزوماً در عرصه سایبری فعالیتی ندارند، در مقابل جاسوسی صنعتی و حملات سایبری امن شوند. در این زمینه، در راهبرد سایبری بسیاری از کشورها از جمله تمامی کشورهای عضو ناتو، یکی از اصول محوری، همکاری گسترده بین دولت با بخش خصوصی و صنعت است که هدف آن در سه حوزه ارتقاء بخش خصوصی سایبری قوی، ایجاد و افزایش امنیت سایبری صنایع حساس و مهم و کمک‌گرفتن دولت از دانش و تجربه بخش خصوصی قابل اشاره است.

۵. تدوین و توسعه حقوق داخلی سایبری

یکی از مهم‌ترین خلأهای موجود حقوقی در بسیاری از کشورها از جمله ایران، در زمینه حقوق مرتبط با فضای سایبری است. به هر حال، فضای سایبر به شکلی بر تمامی عرصه‌های زندگی انسانی تأثیر گذاشته و شرایط را چنان تغییر داده که در نتیجه آن حقوق داخلی نیازمند تدوین و توسعه حقوق سایبری است. برای نمونه و بر اساس روند شدیداً افزایشی جرائم سایبری در ایران و سایر کشورها از جمله کلاه‌برداری، توهین و افترا در فضای سایبر و افشای اطلاعات خصوصی و...، پیش‌بینی‌شده است که در چند سال آینده در تمامی کشورها جرائم سایبری با اختلاف گسترده، سایر جرائم را پشت سرگذارند. بر این اساس، تمامی کشورها در راهبرد سایبری خود یکی از اولویت‌ها را تدوین و توسعه حقوق مرتبط با فضای قرار می‌دهند که البته به دلیل ماهیت خاص فضای سایبر کار بسیار مشکلی است. علت اصلی مشکل‌بودن این امر، ماهیت پویا و در حال تحول فضای سایبر است که عملاً کار را برای تدوین حقوق که امری ماهیتاً ایستا است، مشکل کرده است. بر این اساس، پیشنهاد می‌شود مرکز یا نهادی مسئول زیر نظر مجلس شورای اسلامی تشکیل و با حمایتی که از سوی سایر قوا و مراکز می‌شود، خلأهای موجود در حوزه حقوق سایبری شناسایی شوند. در این زمینه می‌توان به راهبرد سایبری سایر کشورها از جمله ایالات‌متحده آمریکا، اسرائیل یا سایر کشورهای عضو ناتو اشاره کرد که در تمام آن‌ها ضرورت توسعه و تدوین حقوق سایبری یکی از ضروریات اصلی شناخته شده و هر کشوری راهکاری برای پرکردن این خلأ اندیشیده است. برای نمونه، در بسیاری از کشورها جرائمی چون کلاه‌برداری سایبری و جاسوسی سایبری دارای تعریف و مجازات مشخص هستند.

٦. همکاری سایبری با متحدان و سایر کشورها

موضوع مهم دیگری که در یک سند سایبری کارآمد و جامع باید به آن دقت کرد، همکاری با سایر کشورها ضمن توجه به خوداتکایی است. این بدان معناست که کشورها برای موفقیت در فضای سایبر باید ضمن تأکید بر توان داخلی، به دنبال همکاری با سایر کشورهای متحد و نزدیک نیز باشند. علت اصلی تمایل به همکاری با سایر کشورها این

است که کمتر کشوری می‌تواند به‌تنهایی و از طریق اقدامات یک‌جانبه و ملی به امنیت لازم دست یابد. در این زمینه می‌توان به آمریکا به‌عنوان فعال‌ترین و پیشگام‌ترین کشور جهان اشاره کرد. در سند راهبرد سایبری وزارت دفاع آمریکا به‌روشنی بیان شده که اقدامات ملی به‌تنهایی در مقابله با تهدیدات فضای سایبری کافی نیستند. به همین دلیل، وزارت دفاع پیشنهاد کرده که دولت آمریکا به‌دنبال ایجاد ائتلاف بین‌المللی برای ایجاد «بازدارندگی سایبری»[۱] باشد. هدف از این کار، ایجاد جبهه‌ای قدرتمند و مسلط در حوزه سایبری است تا هیچ بازیگری به خود اجازه تهاجم سایبری به کشورهای غربی و متحدان آن‌ها را ندهد و یا در غیر این‌صورت، با پیامدهای ویرانگری مواجه شود. در واقع، همکاری آمریکا با سایر کشورهای غربی در چارچوب ناتو و تدوین سند راهبرد سایبری ناتو در این راستا قابل فهم است.

ضمن اینکه تجربه سایر کشورها نیز به‌خوبی همین امر را تائید می‌کند که صرف دفاع ملی در برابر تهدیدهای برآمده از فضای سایبر نمی‌تواند کارآمد باشد. برای نمونه، در اکثر موارد حملات سایبری علیه ایران، شناسایی ویروس‌ها و بدافزارها نتیجه همکاری با سایر کشورها به‌ویژه روسیه بوده است. در این زمینه در بیشتر موارد ویروس‌ها توسط شرکت‌های خارجی از جمله «کسپرسکی»[۲] شناسایی شده‌اند. ضمن اینکه مسئله فقط لزوم همکاری کشورها در مقابله با تهدیدات سایبری برآمده از سایر کشورها نیست. در شرایط کنونی این نیاز به‌خصوص در مورد سایر تهدیدهای سایبری که منشأ آن‌ها سایر بازیگران به‌ویژه تروریست‌ها، سازمان‌های جنایتکار بین‌المللی، هکرهای فردی و گروهی و حتی افراد هستند نیز وجود دارد.

---

۱. Cyber Deterrence

۲. Kaspersky

نتیجه‌گیری

واقعیت این است که فضای سایبر اهمیت بسیاری در قدرت، امنیت و جایگاه کشورها در سلسله‌مراتب قدرت جهانی پیدا کرده است. اهمیت فضای سایبر چنان است که بسیاری از کشورها در حال تدوین چهارمین یا پنجمین راهبرد سایبری خود هستند. این در شرایطی است که بسیاری از کشورها یا راهبرد سایبری مشخصی ندارند یا اگر دارند، چندان مشخص نیست که کارآمدی و نتایج، موفقیت‌ها و ناکامی‌های آن چگونه سنجیده می‌شود. در این راستا، ضروری است زمینه برای تدوین راهبرد سایبری منسجم، کارآمد و از همه مهم‌تر قابل عملیاتی‌شدن فراهم گردد. در این راهبرد باید ساختار سایبری کشور، میزان و چگونگی سرمایه‌گذاری در حوزه پژوهش و علم‌گرایی سایبری، چگونگی حمایت و همگرایی بین بخش دولتی و خصوصی و تدوین و توسعه حقوق سایبری کارآمد مشخص شود. همچنین، باید نهاد یا مرکزی برای سنجش میزان پیشرفت‌ها یا ناکامی‌ها ایجاد شود تا با رصد همیشگی، مانع از دست رفتن زمان شد. به هر حال، آنچه در آینده نه چندان دور رقابت میان کشورها را شکل خواهد داد، تلاش برای تبدیل‌شدن به قدرت سایبری یا ابرقدرت سایبری جهانی یا منطقه‌ای است.