چالش‌ها و آسیب‌پذیری‌های جمهوری اسلامی ایران در فضای سایبر

قاسم ترابی*

مقدمه

در شـرایط کنونی که امنیت فضـای سـایبر برای کشـورهای مختلف از اهمیت بسـیار زیادی برخوردار اسـت، برای دریافتن فرصـت ها و دفع تهدیدهای آن، باید راهبرد جامع، به روز و پویایی داشـت. داشتن راهبردی این‌چنینی نیز مستلزم شناخت فضای سایبر و آسیب پذیری های اصـلی کشـور در این فضـاسـت. بر این اسـاس، راهبردی می‌تواند موفق باشـد که طراحان آن حداقل بر سـه حوزه تسـلط داشـته باشـند؛ ۱. شـناخت عمیق، ماهیت محور، روندمحور و دوراندیش از فضـای سـایبر؛ ۲. آگاهی از آسـیب پذیری های اصـلی کشور در حوزه سایبری و تلاش برای پوشـش و تقویت آن‌ها؛ ۳. آشـنایی با انواع تهدیدهای سایبری و چگونگی ترکیب تهدید با آسـیب پذیری و تلاش برای شـناخت و اجرای راه‌کارهای مقابله‌ای با آنها. با وجود اهمیت این موضـوع، سـؤال اصـلی این نوشـتار این است که مهم ترین آسیب پذیری جمهوری اسـلامی ایران در حوزه سـایبر کدامند؟ نویسـنده این نوشـتار معتقد است با توجه به روندها و رویدادهای گذشـته و تجربه سـایر کشـورها، پیچیدگی و مشـکل‌بودن شـناخت فضـای سایبر، کاربربودن در تمامی عرصـه‌ها، ضـعف در اعتماد عمومی نسـبت به دولت در حوزه سـایبری،

* دانشیار روابط بین‌الملل، واحد همدان، دانشگاه آزاد اسلامی، همدان، ایران. ghasemtoraby@yahoo.com

نداشتن راهبرد جامع و کارآمد سایبری و جزیره‌ای عمل‌کردن و همگام‌نبودن با فضای انقلاب سایبری از جمله مهم‌ترین آسیب‌پذیری‌ها و چالش‌های کشور در حوزه سایبر هستند.

الف. پیچیدگی فضای سایبر و نگاه سنتی به امنیت

البته این چالش اختصاص به جمهوری اسلامی ایران ندارد و تمامی کشورها در سطوح مختلف با آن مواجه هستند. برای نمونه، در راهبرد سایبری وزارت دفاع آمریکا بر چنین چالشی تأکید شده و راه‌کارهایی برای پوشش آن ارائه شده است.[1] ریشه این چالش به ماهیت این فضا و رویکرد سنتی دولت‌ها نسبت به مقوله امنیت برمی‌گردد. فضای سایبر فضای ابهام، پیچیدگی، پویایی و غیرقابل‌پیش‌بینی است. در چنین فضایی، لزوماً کنترل در دست دولت‌ها نیست و چندان روشن نیست که چه چیزی فرصت و چه چیزی تهدید است. برای نمونه، هنوز مشخص نیست چگونه می‌توان شبکه‌های اجتماعی را گسترش داد و ضمن بهره‌برداری از آنها، تهدیدات رو به گسترش‌شان را نیز مدیریت کرد. همچنین، مشخص نیست فضای سایبر دقیقاً به کجا می‌رود و در کوتاه‌مدت و بلندمدت چه فرصت‌ها و تهدیدهایی را برای کشورها ایجاد می‌کند. ضمن اینکه مشکل بعدی در زمینه ساخت نرم‌افزارها و البته بدافزارها است. مشکل در این حوزه این است که در صورت داشتن دانش، هر کسی می تواند هر چیزی را که بخواهد طراحی کند. همین بدافزارها سالانه میلیاردها دلار برای کشورهای مختلف هزینه دارند. نگرانی از این وضعیت به اندازه‌ای است که کارشناسان سایبر در مورد خارج‌شدن این فضا از کنترل هشدار می دهند. برای نمونه، اخیراً نگرانی جدی در هوش مصنوعی ایجاد شده که بر اساس برآورد برخی کارشناسان، می‌تواند در آینده تهدید جدی امنیتی برای همگان ایجاد کند.

مشکل بعدی در حوزه شناخت فضای سایبر، تسلط رویکرد سنتی به امنیت در بیشتر کشورهاست. رویکرد سنتی به امنیت به شدت نظامی‌زده است که تهدیدها را بیشتر بر محور دولت‌ها ارزیابی می‌کند و فاقد ظرافت و دقت لازم برای شناخت تهدیدهای موجود در فضای سایبر است. نگاه سنتی به امنیت بیشتر بر حذف کامل تهدید تمرکز دارد، این در حالی است که

1. The DoD Cyber Strategy (2015), http://www.defense.gov/home/features/2015/0415_cyber strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf

در فضای سایبر فرصت و تهدید در کنار هم هستند. چنین مشکلی خود را در تهدیدانگاری کل فضـای سـایبر و تلاش برای همراه‌نشدن با آن یا همراهی از طریق اعمال محدودیت‌هایی مانند سرعت پایین اینترنت و فیلترینگ گسترده نشان داده است؛ که نتیجه آن نیز عقب‌ماندن ایران در حوزه دانش سـایبری، ضـعف گسـترده در زمینه تولید نرم‌افزار و سـخت‌افزار و در یک کلام، کاربرشدن در این فضاست. همین امر یکی از دلایل اصلی وابستگی امروز ایران به نرم‌افزارها و سخت‌افزارهای خارجی و جولان شبکه‌های اجتماعی خارجی در کشور و فقدان اعتماد عمومی به نرم‌افزارهای داخلی است.

ب. کاربربودن فضای سایبر

معمولاً کاربربودن به اسـتفاده افراد از نرم‌افزارها و سـخت‌افزارها و به طور کلی، اسـتفاده از فضای سایبر گفته می‌شود. با این حال، به نظر می‌رسد می‌توان از این اصطلاح برای بسیاری از کشـورها نیز اسـتفاده کرد که بیشتر کاربران فضای سایبر هستند. در واقع، بسیاری از کشورهای جهان در محیطی فعال هسـتند که خود کمترین نقشـی در ایجاد و مدیریت کلان آن ندارند و برای آنها، فعالیت در این حوزه مانند بازی در زمین حریف بر اساس ساختار، قواعد و مقرراتی اسـت که کمترین نقش را ایجاد و تدوین آن داشـته‌اند. این کشـورها نگرانی‌های امنیتی جدی نسـبت به این موضـوع دارند. چنین نگرانی‌هایی حتی برای متحدان آمریکا در اروپا نیز ایجاد شـده و بسیاری از آنها خواهان انتقال بخشی از سرورهای شبکه ها به اروپا هستند. اینکه برخی از کشـورها به دنبال داشـتن اینترنت ملی با اسامی مختلف مثل شبکه ملی اطلاعات هستند، نیز در این چارچوب قابل درک اسـت. ایران نیز در این مورد نگرانی‌های عمیق و جدی دارد و در این راسـتا اقداماتی مانند فیلتر برخی شـبکه های اجتماعی خارجی و راه‌اندازی شـبکه ملی اطلاعات را در پیش گرفته اسـت. با این حال، چندان مشـخص نیست این گونه اقدامات تا چه میزان می‌تواند آسیب‌پذیری‌ها را کاهش دهند و همزمان مانع استفاده از فرصت‌ها نیز نشوند.

معنای دیگر کاربربودن، به اسـتفاده گسـترده یک کشـور از نرم‌افزارها و سـخت‌افزارهای خارجی اشـاره دارد. در این زمینه، ایران یکی از کاربران وابسته به نرم افزارها و سخت‌افزارهای خارجی است. برای نمونه، تقریباً تمامی گوشی‌ها و کامپیوترها، فلش‌ها، سی‌دی و دی‌وی‌دی‌ها

و تمامی وسایل خانگی دیجیتال وارداتی هستند که ممکن است آلوده به بدافزارهای جاسوسی و مخرب باشند. در این زمینه می‌توان به گزارش شرکت کسپرسکی در اواخر سال ۹٤ اشاره کرد. در این گزارش آمده است که دستگاه‌های اطلاعاتی آمریکا راهی برای نصب تجهیزات تجسسی و خرابکاری در کامپیوترها و شبکه‌های اطلاعاتی کشورهای مختلف از جمله ایران، روسیه و برخی دیگر از کشورهای آسیایی یافته‌اند. ضمن اینکه بر اساس تحقیقات کسپرسکی، نزدیک به نیمی از موبایل های کاربران ایرانی به بدافزارها آلوده شده‌اند. بر این اساس، کاربربودن جمهوری اسلامی ایران در فضای سایبری، یکی از جدی‌ترین آسیب‌پذیری‌های کشور است که باید برنامه‌ای بلندمدت و چندجانبه برای آن داشت. حمایت از بخش خصوصی برای ایجاد خلاقیت و نوآوری، حمایت از استارت‌آپ‌های ایرانی که در حال حاضر نیز چند نمونه از آن‌ها فعال و موفق هستند و آموزش و تربیت نخبگان سایبری در همه حوزه های مرتبط، از اقدامات پایه‌ای برای داشتن آینده‌ای روشن در فضای سایبر است.

ج. ضعف اعتماد به دولت در حوزه سایبری

یکی دیگر از چالش‌های جمهوری اسلامی ایران در فضای سایبر، ضعف اعتماد عمومی به دولت در این عرصه است که بیشتر در بی‌اعتمادی عمومی نسبت به شبکه های اجتماعی داخلی و استفاده گسترده از فیلترشکن‌ها تجلی یافته است. یکی از نگرانی‌های اصلی در این زمینه، استفاده گسترده از شبکه های اجتماعی خارجی مانند تلگرام است که امکان رصد روندها و رویدادهای داخلی و شناخت ارزش ها، باورها و خواسته های عمومی مردمان ایران را برای کشورهای دیگر فراهم آورده است. به هر حال، شبکه های اجتماعی محل مناسبی برای آگاهی از تحولات اجتماعی، ارزشی، دینی و فرهنگی یک جامعه به‌ویژه جامعه ایران هستند. در چنین شرایطی، حجم بسیار وسیع و گسترده فعالیت ایرانیان در تلگرام و سایر شبکه های اجتماعی، ضمن فرصت‌سازی، می‌تواند زمینه آسیب‌پذیری کشور را نیز فراهم کند. تصمیم حاکمیت مبنی بر فیلتر تلگرام بر همین اساس بوده، که البته در عمل به نظر می رسد نه تنها نتیجه مورد انتظار را تأمین نکرد، بلکه بر اساس آمار و ارقام موجود، بر میزان استفاده از فیلترشکن‌های چندین برابر افزوده شده است. در حال حاضر، در ایران کمتر موبایل هوشمندی وجود دارد که حداقل

یک فیلترشکن فعال روی آن نصب نباشد. لازم به اشاره است که استفاده از فیلترشکن باعث افزایش احتمال رصد اطلاعات داخلی توسط بازیگران خارجی می شود؛ ضمن اینکه مشکلات جدی را برای سرعت و کیفیت اینترنت نیز به وجود آورده است.

به هر حال، باید میان استفاده از فرصت های شبکه های اجتماعی و تهدیدهای ناشی از آن راهی پیدا کرد که ضمن بهره‌گیری از فرصت‌ها، با تهدیدها نیز مقابله شود. ترمیم و ارتقای اعتماد در روابط جامعه و حکومت، شرط اساسی و اولیه نیل به چنین مسیری است. در واقع، تا زمانی که این ارتباط مبتنی بر بی‌اعتمادی باشد، سیاست‌های محدودکننده در فضای سایبر نه تنها کارآمد نخواهد بود، بلکه ممکن است بر مشکلات موجود بیفزاید.

د. نداشتن راهبرد جامع و کارآمد سایبری و جزیره‌ای عمل‌کردن نهادهای متولی

نداشتن راهبرد جامع و کارآمد از جدی‌ترین چالش‌های کشور در حوزه سایبری است. البته این بدان معنا نیست که ایران اسناد سایبری ندارد، بلکه مشکل اصلی نبود زمینه لازم در کشور برای تدوین و مهم تر از آن، اجرای راهبرد سایبری جامع و کارآمد است. ضعف اصلی در این زمینه، به ورود دیرهنگام ایران در تمامی ابعاد و در تمامی سطوح به فضای سایبر و همگام‌نبودن دولت و جامعه با انقلاب سایبری برمی گردد. در واقع، همان‌گونه که در مورد ورود سایر تکنولوژهای جدید نیز دیده می‌شود، دولت و جامعه ایرانی با وجود داشتن قواعد و مقررات کافی، در اجرا با مشکل مواجه هستند. به هر حال، چنین مسئله‌ای باعث جزیره‌ای عمل کردن نهادهای مختلف متولی حوزه سایبر در ایران شده و این آسیب پذیری بزرگی است. در چنین شرایطی، کشور ما نیازمند راهبردی جامع و کارآمد است که مبتنی بر برنامه‌ای بلندمدت و جامع بر محور شناخت فضای سایبر، شناخت فرصت ها و تهدیدها و طرح ریزی برای همه بخش‌ها اعم از بخش دولتی و خصوصی باشد.

در این راهبرد باید در مورد تهدیدها، فرصت‌ها، معرفی اصلی‌ترین نهاد مسئول و پاسخ‌گو در مدیریت سایبری کشور، ایجاد مراکز علمی و پژوهشی سایبری، تربیت نیروی نخبه سایبری، آموزش سایبری از ابتدایی تا دانشگاه، تقسیم وظایف بین مراکز اصلی و فرعی سایبری در کشور، ایجاد هماهنگی بین نهادها و مراکز فعال سایبری، همکاری دولت با دانشگاه ها و بین بخش

خصوصی و صنعت، همکاری بین المللی سایبری، تدوین قواعد و مقررات سایبری و برگزاری مانورهای سایبری سالیانه بحث شود و برنامه‌های عملیاتی در این موارد تدارک دیده شود.

هـ همگام‌نبودن با فضای انقلاب سایبری

همگام‌نبودن ساختار اداری و اجرایی، مدیران و کارکنان دولتی و همچنین بخش خصوصی و از همه مهم تر نیروهای نظامی و دفاعی با انقلاب سایبری، مشکل بعدی است. مسئله اصلی در این زمینه، ساختار مدیریت کشور است که همچنان بر مدار مدیریت سنتی گذشته می چرخد. این در شرایطی است که در کشورهای پیشرفته، ساختارهای سیاسی، نظامی و امنیتی اصلاحات جدی را در راستای همراه‌شدن با انقلاب سایبری به اجرا گذاشته‌اند. برای نمونه، سازمان اطلاعات مرکزی آمریکا (سیا) چندی پیش اصلاحاتی جدی را برای هماهنگی با چالش‌ها و تهدیدهای سایبری در اولویت قرار داد؛ از جمله اینکه در این سازمان، مراکزی فعال در حوزه سایبری ایجاد شدند و وظیفه هرکدام از آن‌ها و روش همکاری و هماهنگی آن‌ها با سایر مراکز دولتی و غیردولتی مشخص شده است. موضوع مهم دیگر، جذب نیروهای کارآمد در حوزه سایبری و البته آموزش های جدی کارکنان استخدام‌شده برای همراه شدن با انقلاب سایبری است. در این زمینه، در سازمان سیا هرساله دوره‌های کوتاه و میان‌مدت آموزش سایبری برای کارکنان در نظر گرفته شده است. همچنین، این سازمان بهترین نخبگان سایبری آمریکایی و حتی غیر آمریکایی را دعوت به همکاری می‌کند. اقدام دیگر سیا، همکاری با شرکت‌های فعال آمریکایی در فضای سایبر است.

بر این اساس، در ایران نیز لازم است ساختار اداری و اجرایی مطابق با انقلاب سایبری به‌روز شوند و کارمندان و کارکنان دولتی، به‌ویژه در مراکز سیاسی، نظامی و امنیتی، آموزش‌های جدی و حرفه‌ای برای فعالیت و بهره‌برداری از فضای سایبر کسب کنند.