ارزیابی ناامنی سایبری در منطقه خاورمیانه و پاسخ دولت‌ها

سید حامد حسینی [۱]

[۱] دانشجوی دکتری روابط بین‌الملل، دانشگاه گیلان، رشت، ایران
hamedhoseini@ut.ac.ir

چکیده

تهدیدات سایبری یک پدیده‌ی جهانی است که با وجود پیشرفت در فناوری‌ها و عملکرد امنیت سایبری، به طور مداوم در حال پیچیده‌تر شدن و تأثیرگذاری بیشتر است. مسائل امنیت سایبری وابسته به عوامل چندوجهی گوناگونی هستند: وابستگی فزاینده به فناوری اطلاعات برای عملکردهای گوناگون، ویژگی‌های رفتار بازیگران سیاسی که منجر به منازعه و جنگ می‌شود و آسیب‌پذیری‌های فناوری اطلاعات که باعث اختلال در عملکرد می‌شوند. در این مقاله به این سؤال اساسی پرداخته می‌شود: با توجه به منابع اصلی ناامنی سایبری در منطقه دولت‌ها چگونه به این چالش پاسخ داده‌اند؟ این مقاله در ابتدا طیفی از عوامل تهدید سایبری را در داخل و خارج از منطقه و همچنین عوامل ساختاری که باعث ناامنی سایبری می‌شوند را برجسته می‌کند. در ادامه به پاسخ‌های دولتی پرداخته می‌شود که به نوبه خود طیفی از واکنش‌ها را در بر می‌گیرد. این نوشتار با تکیه بر رویکرد واقع‌گرایی و روش توصیفی-تحلیلی به دنبال اثبات این فرضیه است که دولت‌های منطقه به عنوان بازیگران اصلی، پاسخ‌های متفاوتی به ناامنی سایبری داده‌اند. در سطح ملی، برخی دولت‌ها به دنبال افزایش ظرفیت امنیت سایبری بوده‌اند و تغییرات مهم نهادی و اداری همچون دفاع دیجیتالی و ادغام در قابلیت‌های نظامی را در اولویت خود قرار داده‌اند. در سطح بین‌الملل نیز برخی از کشورهای منطقه در مذاکرات پیرامون هنجارهای سایبری بین‌الملل شرکت کرده‌اند، در حالی که برخی دیگر از بازیگران منطقه‌ای خارج از این روند هستند. نتایج این مقاله مبتنی بر چند توصیه در سطح سیاست‌گذاری ملی و نیز بر اساس تغییرات سایبری در منطقه استوار است.

کلمات کلیدی: امنیت سایبری، واقع گرایی، خاورمیانه، تهدید، دولت.

۱ مقدمه

ما در عصری از فناوری‌های پیچیده‌تر و پشتیبانی از تغییرات گسترده‌تر زندگی می‌کنیم. انقلاب صنعتی چهارم فرصت‌های اقتصادی و اجتماعی عظیمی را برای مردم، سازمان‌ها و دولت‌ها به ارمغان آورده است. افزایش قابل توجه اتصال به اینترنت، رشد بالای تعداد دستگاه‌های متصل به شبکه و استفاده سریع از فناوری‌هایی مانند محاسبات ابری، روباتیک پیشرفته و هوش مصنوعی اساساً زندگی مردم را تغییر داده است. آن‌ها همچنین شیوه تجارت سازمان‌ها و نحوه ارائه خدمات دولتی و تعامل با شهروندان را تغییر می‌دهند.

درعین‌حال، با هر سیستم یا دستگاه جدیدی که به اینترنت متصل است، دامنه آسیب‌های سایبری و پیامدهای حملات موفقیت‌آمیز افزایش می‌یابد. همان‌طور که مهاجمان سایبری در عملیات خود پیچیده‌تر می‌شوند، سیاست‌گذاران نیز در تلاش‌اند تا واکنش‌های مناسب را ارائه دهند.

فضای سایبری به‌عنوان محیطی برای تعامل دولت‌ها، پیامدهای عمیقی برای امنیت بین‌المللی ایجاد کرده است. از یک‌سو، فضای سایبری فرصت‌هایی را برای کشورها فراهم کرده است تا در زمینه همکاری‌های نظامی و اطلاعاتی همکاری مؤثرتری داشته باشند. از سوی دیگر، رواج فضای سایبری باعث ایجاد تهدیدات منحصربه‌فردی شده است که نیازمند پاسخ‌های مستقیم سیاست‌گذارانه از سوی تصمیم‌گیرندگان است. درحالی‌که این فعل‌وانفعالات همچنان بر رفتار دولت‌ها تأثیر می‌گذارد، اما پیشرفت اندکی در مطالعه این موضوعات حیاتی حاصل شده است زیرا مشخص نیست که آیا نظریه‌ها و توضیحات موجود قادر به تفسیر پدیده‌های سایبری هستند یا خیر (Kello, 2013). امنیت سایبری ذاتاً بین‌رشته‌ای است و بیشتر فعالیت‌ها در یک حوزه بلافاصله بر سایر حوزه‌ها تأثیر می‌گذارد. فن‌آوری‌ها و تکنیک‌ها، استراتژی‌ها و تاکتیک‌ها، انگیزه‌ها و ایدئولوژی‌ها، قوانین، نهادها و صنایع، قدرت و پول و در یک کلام همه این موضوعات در امنیت سایبری نقش دارند و همه این‌ها به‌شدت درهم‌تنیده شده‌اند. مسائل مربوط به امنیت سایبری هم جهانی هستند، به این دلیل که به زیرساخت‌های فراملی بستگی دارند و پارادایم‌های جغرافیایی سیاست بین‌الملل را تغییر می‌دهند؛ و نیز موضوعی هستند، زیرا در زمینه‌های مختلف اجتماعی، ملی و منطقه‌ای متفاوت ظاهر می‌شوند؛ بنابراین امنیت سایبری ازجمله در خاورمیانه و شمال آفریقا[1] یک مسئله چندوجهی است و چگونگی پاسخ دولت‌ها به این ناامنی‌های سایبری مطمح نظر هست.

این تحقیق در پی آن است تا از امنیت سایبری به‌عنوان یک هدف برای تمرکز بر مواجهه با ناامنی سایبری بهره گیرد. یکی از واضح‌ترین جنبه‌های ناامنی سایبری در منطقه خاورمیانه، طیف وسیع تهدیدها است که از عملیات هکرها تا نگرانی‌های مربوط به باندهای جنایتکار و جاسوسان که در فضای مجازی عمل می‌کنند را در بر می‌گیرد. این مقاله استدلال می‌کند که منابع ساختاری و عوامل کلیدی ناامنی سایبری در سراسر منطقه خاورمیانه مشترک است و زمینه‌ای برای اقدامات مشترک را فراهم می‌کند. بعد دیگر تحقیق بر دولت‌ها به‌عنوان محلی برای پاسخ به این منابع ناامنی متمرکز است. در بسیاری از موارد، اقدامات دولتی برای رفع چنین ناامنی‌های سایبری بدون همکاری گسترده‌تر بخش‌های اقتصادی یا تغییرات اجتماعی، ناکافی یا حتی نامناسب است. بااین‌وجود، دولت‌ها کلید پاسخ‌های امنیت سایبری هستند زیرا تجربیات در سراسر جهان نشان داده است که رویکردهای مناسب، چه در مقررات رسانه‌های اجتماعی علیه شبکه‌های نفوذ و چه تشویق شرکت‌ها به رفع نقص داده‌ها، بدون حمایت یا مداخله دولت پیشرفت چندانی ندارد. از سوی دیگر ادبیات مطالعات سایبری در دهه‌های گذشته به‌طور قابل توجهی افزایش یافته است. بااین‌حال، تحقیقات در مورد منازعه سایبری و موضوعات مرتبط بسیار خاص، متمایل به سیاست‌گذاری است و لزوماً به ایجاد یا آزمایش تئوری‌های مرکزی برای مطالعه روابط بین‌الملل کمک نمی‌کند. در ادبیاتی که می‌توان آن را علمی در نظر گرفت، بیشتر مطالعات بر روی بازیگران قدرتمند، به‌ویژه رقابت بین چین، ایالات متحده و روسیه

[1] MENA: the Middle East and North Africa

متمرکز شده است. علیرغم مشارکت فعال سایر دولت‌ها در فضای سایبری، ارتباط دولت‌های خاورمیانه در چالش‌های سایبری تا حد زیادی نادیده گرفته شده است.

استدلال مشخص مقاله این است که علیرغم ناامنی‌های مشترک در فضای سایبری، دولت‌های منطقه خاورمیانه با توجه به اولویت‌های سیاسی متفاوت، واکنش‌های قابل توجهی را اتخاذ کرده‌اند. برخی توسعه نهادی قوی و متمرکز را برای امنیت موثر سایبری مهم می‌دانند، درحالی‌که برخی دیگر مسئولیت و توانایی را بین سازمان‌های بین دولتی تقسیم کرده‌اند. به‌طور مشابه، در سطح بین‌المللی، برخی از دولت‌ها به‌طور گسترده در مذاکرات حکمرانی امنیت سایبری مشارکت داشته‌اند، درحالی‌که برخی دیگر از این مسیر جدا شده‌اند و فاصله گرفتن از این فرایندها را بهترین راه خود برای اطمینان از انعطاف‌پذیری و حفظ حاکمیت می‌دانند. این مقاله پیرامون دو مسئله تحقیق سازمان یافته است. بخش اول منابع ناامنی سایبری در منطقه خاورمیانه را مورد بررسی قرار می‌دهد و سپس عوامل ساختاری را بررسی می‌کند. بخش دوم به پاسخ‌های دولتی می‌پردازد و به‌نوبه خود به پاسخ‌های بین‌المللی نیز می‌پردازد. این مقاله با چندین توصیه در عرصه سیاست‌گذاری بر اساس تغییرات اخیر در همسویی سیاسی در منطقه به پایان می‌رسد.

۲ منابع ناامنی سایبری مبتنی بر بازیگران

منابع امنیت سایبری مبتنی بر بازیگران در منطقه خاورمیانه را می‌توان در سه نوع اصلی طبقه‌بندی کرد: رقابت و درگیری بین دولتی، زمینه‌های حملات و جنگ‌های داخلی و جرائم سایبری که به ترتیب توضیح داده خواهند شد. اول، منطقه خاورمیانه از وضعیت جاسوسی سایبری به‌عنوان ابزاری برای پیشبرد منافع منطقه‌ای مستثنا نیست. شرکت‌های امنیت سایبری، کمپین‌های جاسوسی سایبری را با هدف قرار دادن نهادهای دولتی و خصوصی در تعدادی از کشورهای خاورمیانه و همچنین عملیات جاسوسی سایبری قدرتمند از سوی قدرت‌های بزرگ و فرامنطقه نسبت داده‌اند.

به‌عنوان نمونه، پس از افشای عملیات خرابکارانه موسوم به استاکس نت[۲] در سال ۲۰۱۰ علیه برنامه هسته‌ای ایران، عملیات سایبری مختل‌کننده دولتی به دلیل تنش‌ها در خلیج فارس شروع شد؛ ازجمله عملیات علیه زیرساخت‌های حیاتی در عربستان از سال ۲۰۱۲ (ازجمله بدافزار "Shamoon"). حملات سایبری ایالات متحده در پاسخ به تحرکات ایران در سال ۲۰۱۹ و گزارش حملات سایبری مستمر بین اسرائیل و ایران در سال ۲۰۲۰ (Harknett, 2020). خلیج فارس همچنین بر کمپین‌های نفوذ دولتی تمرکز کرده است زیرا بحران خلیج فارس در سال ۲۰۱۷ با ایجاد فضای رسانه‌ای تفرقه‌انگیزی تشدید شد به‌ویژه با دست‌کاری رسانه‌های اجتماعی تحت حمایت دولت‌ها علیه قطر و ترکیه. همچنین کشته شدن جمال خاشقچی در کنسولگری عربستان در استانبول در سال ۲۰۱۸ به تامین کنندگان خصوصی نرم‌افزارهای نظارتی هدفمند و همچنین تأثیرگذاری بر کمپین‌های رسانه‌های اجتماعی مرتبط بود (Timberg, 2021).

دوم، گذشته از این اختلافات بین دولتی، فعالیت‌های مشابهی نیز در زمینه جنگ داخلی توسعه پیدا کرده است. ابزارهای جاسوسی سایبری به بسیاری از بازیگران در جنگ داخلی سوریه نسبت داده شده است

[2] Stuxnet

که مهم‌ترین آن‌ها ارتش الکترونیکی سوریه[3] وابسته به حکومت اسد است (Baezner, 2017). اعضای ائتلاف بین‌المللی در سوریه ادعا کرده‌اند که عملیات سایبری علیه داعش[4]، هم برای بر هم زدن تبلیغات و هم برای حمایت از اقدامات نظامی انجام شده است.

در جنگ داخلی لیبی اطلاعات غلط فراوانی وجود داشته است؛ بسیاری از طرفین درگیری تبلیغات رسانه‌های اجتماعی را انجام می‌دهند و همچنین کمپین‌های رسانه‌های اجتماعی از طرف شرکت‌های رسانه‌ای مرتبط با کشورهای خارجی مانند روسیه، مصر و امارات تغذیه می‌شوند. گزارش شده است که برخی از شرکت‌های نظامی خصوصی درگیر در این درگیری قابلیت‌های حمله سایبری را نیز ارائه می‌دهند (Grossman, 2020). به‌طور کلی، هم جنگ داخلی و هم اختلافات سیاسی طولانی‌مدت، بستر مستمری را برای حملات سایبری در منطقه فراهم کرده‌اند، زیرا بازیگران غیردولتی از طریق تخریب و هک و نشت به دنبال بالا بردن تنش در موضوعات مختلف سیاسی مانند درگیری اسرائیل/فلسطین و تنش‌های عربستان و ایران بوده‌اند.

سوم، طیف وسیعی از بازیگران مخرب از ابزارهای سایبری برای سود مالی نامشروع استفاده می‌کنند. درحالی‌که این بازیگران در سراسر جهان فعالیت می‌کنند، اتفاقات قابل توجهی توسط بازیگران منطقه رخ داده است و همچنین اثرات دامنه‌داری از این حملات در سراسر جهان وجود دارد. به‌عنوان نمونه، دو مورد مجزا از سرقت اطلاعات کارت اعتباری مشتریان بانک مسقط عمان و RAKBank امارات در دسامبر ۲۰۱۲ و فوریه ۲۰۱۳ وجود داشت. این اطلاعات در اختیار یک شبکه جنایی فراملی قرار گرفته بود که ۴۵ میلیون دلار پول نقد از دستگاه‌های خودپرداز در سراسر جهان با استفاده از اطلاعات کارت برداشت کرده است. در سال‌های بعد، چندین نوع بدافزار برنامه‌های بانکداری تلفن همراه در امارات را نیز هدف قرار دادند (Sun, 2017). جرائم مالی آنلاین همچنین افراد را هدف قرار می‌دهند و دارای سوگیری جنسیتی قابل توجهی است. به‌عنوان مثال، باج‌خواهی به دنبال به اشتراک‌گذاری تصاویر خصوصی، جنبه مهم اما ناشناخته‌ای از امنیت سایبری در سطح شخصی و خانوادگی است تا عرصه دولتی.

۳ منابع ساختاری ناامنی سایبری

ما همچنین می‌توانیم منابع ساختاری ناامنی سایبری را به سه نوع اصلی طبقه‌بندی کنیم. اولین مورد از نظر شرایط ژئوپلیتیکی است زیرا منطقه خاورمیانه تحت تأثیر متغیر رقابت تجاری و فناوری ایالات متحده و چین قرار گرفته است. از یک سو، بسیاری از کشورهای خاورمیانه ازجمله ترکیه، اسرائیل و بازیگران حوزه خلیج فارس روابط نزدیک امنیتی و دفاعی با آمریکا و متحدانش دارند؛ از سوی دیگر، سرمایه‌گذاری‌های چین در زیرساخت‌ها، مشارکت‌ها در بخش انرژی و تحقیقات در زمینه‌های مرتبط با فناوری 5Gو هوش مصنوعی (AI)[5] برای این کشورها بسیار جذاب است؛ بدین لحاظ، آن‌ها به دنبال ایجاد تعادل بین همکاری اقتصادی چین و الزامات امنیتی ایالات متحده بوده‌اند (Hakmeh, 2020).

[3] SEA: Syrian Electronic Army
[4] ISIS: the Islamic State of Iraq and Syria
[5] Artificial Intelligence

تحولات ژئوپلیتیک از جهات دیگر بر امنیت سایبری خاورمیانه تأثیر می‌گذارد. به‌عنوان مثال، تقویت قوانین حفاظت از داده‌های اتحادیه اروپا از طریق مقررات عمومی حفاظت از داده‌ها (GDPR)[۶] باعث شده است که شرکت‌ها و اشخاص حقوق مشابهی را در جاهای دیگر مورد پی‌جویی قرار دهند و همچنین الزامات محلی سازی داده‌ها و مقررات محاسبات ابری[۷] را در سراسر منطقه، به‌ویژه در خلیج فارس، منعکس کنند (Ali, 2016). سرانجام، شکاف‌های ژئوپلیتیکی از طریق توسعه زیرساخت‌های واقعی اینترنت در منطقه به شکل فیزیکی خود را نشان می‌دهد. بازسازی زیرساخت‌های دیجیتالی پس از جنگ‌های داخلی در سوریه، لیبی و یمن و همچنین ایمن‌سازی پروژه‌های جدید شهری مانند Neomدر عربستان سعودی، پیچیدگی را بر رقابت موجود و بهره‌برداری مداوم از پروتکل‌های مسیریابی و کابل‌کشی در منطقه می‌افزاید.

دومین منبع ساختاری ناامنی سایبری مبتنی بر بازار است. مشکلات مهمی در ایجاد ظرفیت‌های امنیت سایبری در منطقه خاورمیانه وجود دارد که ناشی از انگیزه‌های نامطلوب برای بخش خصوصی به‌ویژه در زیرساخت‌های حیاتی است تا اولویت امنیت شبکه‌های دیجیتالی خود را بر سودهای کوتاه‌مدت و قابل اعتماد بیشتر قرار دهد. علاوه بر این، امنیت سایبری از نظر ساختاری به شیوه‌های امنیتی کلیدی مانند آزمایش نفوذ به تحقیقات آسیب‌پذیر وابسته است؛ اما این شیوه‌های امنیتی غیرنظامی می‌تواند برای بهره‌برداری از بخش‌های امنیتی و اطلاعاتی نیز مورد استفاده قرار گیرد و تعدادی از بازیگران در منطقه چنین تحقیقات مشکوکی انجام می‌دهند (DeSombre, 2021). این ویژگی ساختاری پیوندهای تنگاتنگ بین بسیاری از این شرکت‌ها و سازمان‌های نظامی و اطلاعاتی در کشورشان را نمایان می‌کند، بدین معنا که بازار ابزارهای سایبری با تلاش هم‌زمان دولت‌ها برای توانایی‌های امنیتی و جاسوسی خود همپوشانی شده و از آن‌ها پشتیبانی می‌کند.

سومین منبع ساختاری ناامنی سایبری در توسعه رسانه‌های اجتماعی در منطقه خاورمیانه نهفته است. تقریباً همه پلتفرم‌های بزرگ رسانه‌های اجتماعی از ایالات متحده سرچشمه گرفته و مقر آن‌ها در ایالات متحده است، بدین معنی که قوانین تعدیل محتوا و استانداردهای جامع و وسیع‌تری از سوی ایالات متحده یا بازارهای کلیدی مانند اروپا و نه منطقه خاورمیانه ایجاد و اعمال می‌شوند. کشورهایی مانند عربستان سعودی برای دور زدن این محدودیت‌ها از روش‌های غیرمتعارف استفاده کرده‌اند، مانند استخدام افراد داخلی در دفاتر توییتر در کالیفرنیا برای ارائه اطلاعات در مورد حساب‌های خاص (Kantrowitz, 2020). به‌طور گسترده‌تر، اکثر بازیگران منطقه‌ای بر معماری‌های نظارتی در سطح ملی، با حمایت از قوانین گسترده جرائم سایبری، برای نظارت بر رسانه‌های اجتماعی منطبق بر هنجارهای فرهنگی و همچنین محدود کردن بحث سیاسی آزاد، تکیه کرده‌اند. البته شبکه‌های اجتماعی جایگزین توسط جمهوری اسلامی ایران، عربستان سعودی و امارات متحده عربی پیشنهاد و راه‌اندازی شده اما موفقیت چندانی نداشته‌اند.

[6] the General Data Protection Regulation
[7] cloud computing

۴ پاسخ‌های متنوع

این بخش با تمرکز بر اقدامات دولت‌های خاورمیانه در سطح ملی و دوجانبه و سپس مشارکت منطقه در مدیریت امنیت بین‌الملل سایبری در مجامع بین‌المللی و در مورد انواع واکنش‌های دولت به منابع ناامنی سایبری منطقه، اعم از ساختاری یا غیر ساختاری، بحث خواهد کرد. در سراسر منطقه خاورمیانه و فراتر از آن باید تأکید کرد که واکنش‌های دولت اشکال مختلفی دارد، از جمله ابتکارات سیاسی، قانونی و نظارتی. در سطح استراتژیک، ما همچنین می‌توانیم پاسخ‌های دولت را به‌عنوان چندین هدف متمایز، از جمله بازدارندگی (منصرف کردن عوامل تهدیدکننده از هدف قرار دادن آن دولت)، دفاع (بهبود حفاظت و آگاهی از امنیت سایبری، به‌ویژه از طریق ظرفیت‌سازی) و تاب‌آوری (اطمینان از تداوم عملکردهای اصلی دولت با وجود اختلال سایبری) موردنظر و تقسیم‌بندی قرار دهیم؛ اما در عرصه عمل، تمام این استراتژی‌ها و سیاست‌های دولتی در یک مجموعه مرتبط به هم به این اهداف می‌رسند و بنابراین کاملاً متمایز نیستند.

۱.۴ پاسخ‌های ملی و دوجانبه

بر اساس شاخص جهانی امنیت سایبری ITU که در سال ۲۰۱۸ انجام شد، عربستان سعودی، عمان و قطر در زمینه امنیت سایبری سه کشور برتر جهان عرب و در رتبه‌های بعدی مصر، امارات، کویت و بحرین قرار گرفتند (ITU, 2018). این دولت‌ها گام‌های مهمی در جهت ایمن‌سازی دیجیتالی خدمات دولتی برداشته‌اند و امارات متحده عربی از بسیاری جهات از سایر کشورها جلوتر است درحالی‌که سایر دولت‌های خاورمیانه نمرات ضعیف‌تری دارند. بر اساس مطالعه ۲۰۱۹ توسط Google و Bain & Company، بازار تجارت الکترونیک در سال ۲۰۱۷ در منطقه خاورمیانه به‌طور کلی ۳.۸ میلیارد دلار ارزش داشت و در شرایط قبل از همه‌گیری کرونا ۲۵ درصد رشد کرد (Bain&Company and Google, 2019).

این مطالعه، مصر و کشورهای حوزه خلیج را با هم به‌عنوان مرکز سایبری منطقه در نظر گرفته است؛ با توجه به اینکه این کشورها ۸۰ درصد از بازار تجارت الکترونیکی منطقه را به‌طور کلی (به‌استثنای اسرائیل) تشکیل می‌دهند. بر اساس تحقیقات گارتنر در حوزه امنیت سایبری، ارزش فروش تجهیزات امنیت سایبری بین سال‌های ۲۰۱۴ تا ۲۰۱۸ دو برابر شده و به حدود ۲ میلیارد دلار رسیده است (Shetty, 2018). سایر آمار ارقام بالاتری را ارائه می‌دهند که نشان می‌دهد بازار امنیت سایبری خاورمیانه در سال ۲۰۲۰ به ارزش حدودا ۱۶ میلیارد دلار رسیده است (Markets and Markets, 2020).

یک عنصر کلیدی در ایجاد ظرفیت امنیت سایبری، استراتژی امنیت سایبری ملی است. اکثر دولت‌ها در منطقه خاورمیانه، حداقل یک‌بار چنین استراتژی را منتشر کرده‌اند و بسیاری از آن‌ها چندین بار استراتژی‌های خود را به‌روز کرده‌اند. بسیاری از دولت‌های منطقه تلاش‌های گسترده‌ای را در زمینه آموزش امنیت سایبری با ارائه مدارک در زمینه‌های فنی و سازمانی انجام داده‌اند و همچنین راه‌های عملی‌تر برای نقش‌های حرفه‌ای امنیت سایبری و افزایش آگاهی عمومی را بر عهده گرفته‌اند. این دوره‌ها به‌ویژه توسط زنان پذیرفته شده است و جنبه‌های جنسیتی هویت‌های حرفه‌ای و شخصی امنیت سایبری و عوامل ساختار بخش قوی برای ظرفیت‌سازی امنیت سایبری در منطقه خاورمیانه صورت پذیرفته است.

از نظر نهادی، برخی دولت‌های منطقه مسئولیت‌های امنیت سایبری را در یک سازمان ملی امنیت سایبری متمرکز کرده‌اند. کشورهایی که در سال گذشته این کار را انجام داده‌اند عبارت‌اند از عمان، بحرین و قطر؛ درحالی‌که سایر کشورها چندین ترتیبات نهادی مانند شورای عالی امنیت سایبری مصر[۸] یا آژانس ملی امنیت الکترونیکی امارات[۹] (NESA) را تأسیس کرده‌اند. چنین سازمان‌هایی برای ادغام عملکردهای مجازی قبلی که در وزارتخانه‌های ارتباطات و کشور و غیره ادغام شده‌اند، طراحی شده است. حساس‌ترین جنبه این سیاست بوروکراتیک، برای دولت‌های خاورمیانه و همتایان خود در ایالات متحده و اروپا، رابطه بین چنین سازمان‌هایی با سازمان‌های نظامی و اطلاعاتی است. ارزیابی‌ها نشان داده‌اند که چگونه مثلا در ترکیه، این رقابت نهادی منجر به نقش امنیتی غالب در چنین تحولاتی شده است، درحالی‌که دیگران پتانسیل چنین موسساتی را در فضاهای مورد مناقشه مانند گستره فلسطین و اسرائیل نقد کرده‌اند (Unver, 2018).

دولت‌های دیگر مانند تونس، شامل ترتیبات چند ذی‌نفع را که شامل بخش‌های دولتی و خصوصی و نمایندگان جامعه مدنی می‌شود، مطابق با ترتیبات گسترده‌تر چندجانبه در مدیریت جهانی اینترنت دنبال کرده‌اند. به‌طور کلی، به‌استثنای اسرائیل و ایران، سایر دولت‌های منطقه به دلیل عدم وجود ساختارهای سایبری نظامی عمومی و عدم ایجاد دستورات سایبری جداگانه، قابل توجه هستند. این ممکن است به دلیل عدم توانایی به‌طور کلی یا به این دلیل باشد که منبع قدرت سایبری در جای دیگری مانند سازمان‌های اطلاعاتی قرار دارد، یا این‌که این کشورها ترجیح می‌دهند با ایجاد برنامه‌های سایبری تهاجمی، سیگنال‌های جداگانه‌ای را ارسال نکنند (Raymond, 2015).

علاوه بر این، دولت‌ها مشارکت‌های دوجانبه جدید یا تقویت‌شده‌ای را دنبال کرده‌اند که پاسخ‌های امنیت سایبری را در برابر طیف وسیعی از تهدیدات درک شده از مخالفت‌های سیاسی شدید در داخل و خارج تا پیامدهای بالقوه عملیات سایبری علیه زیرساخت‌های حیاتی تسهیل می‌کند. پویایی چنین مشارکت‌هایی عموما از اتحادهای دیپلماتیک وسیع‌تری پیروی می‌کند، اگرچه شکاف شورای همکاری خلیج فارس و سکون نهادی اتحادیه کشورهای عرب چالش‌های پیروی از خطوط سازمانی ایجادشده را آشکار می‌کند. نمونه این مشارکت در تولید امنیت سایبری مثالی بین امارات و عربستان است. اگرچه به‌طور کامل در مورد یمن و دیگر نقاط نبرد سازگار نیست، اما روابط آن‌ها نمونه‌ای چابک برای امنیت سایبری و کنترل اطلاعات است. همکاری امنیت سایبری همچنین می‌تواند به ایجاد ارتباط در خطوط طولانی سایبری کمک کند. به‌عنوان مثال، امضای اخیر توافقنامه ابراهیم و عادی‌سازی روابط اسرائیل با بحرین، سودان، امارات متحده عربی و مراکش به این معناست که بخش قوی امنیت سایبری اسرائیل می‌تواند علیرغم تنش‌ها در زمینه ارزش‌های دموکراتیک، علناً تجربیات خود را به کشورهای خلیج فارس صادر کند (Fakro, 2020). بااین‌حال، سردی کنونی در روابط بین برخی بازیگران ممکن است اتحادها را در جهت دیگری تغییر دهد و این مسئله مانعی برای مشارکت گسترده‌تر است. بدیهی است که همکاری در حوزه امنیت سایبری می‌تواند یک کارت دیپلماتیک مفید برای همه طرف‌ها باشد.

بخشی از دلایل تغییر مسیرهای فوق، به‌ویژه حرکات اسرائیل، مقابله با موفقیت ایران در شیوه بسیار

[8] Egypt's Supreme Cybersecurity Council
[9] the UAE's National Electronic Security Agency

متفاوت همکاری‌های سایبری است. برخلاف بازیگران فوق، ایران در پی برخی ناآرامی‌ها فضای سیاسی و اجتماعی خود طی سال‌های ۲۰۱۷ تا ۲۰۱۹ دست به تعدیل معماری اینترنت داخلی خود در جهت کنترل متمرکز بر آمد تا خودمختاری فنی خود را از زیرساخت اینترنت سایر دولت‌های منطقه افزایش دهد. درعین‌حال، ایران صحنه سایبری قابل توجهی را پرورش داده است، به‌طوری‌که افراد با استعداد در نهادهایی که وظیفه نظامی و اطلاعاتی را بر عهده دارند به کار گرفته است (Anderson, 2018). اگرچه این ممکن است با توجه به منابع محدود ایران راه حلی کارآمد باشد، اما محدودیت بر روی چنین نهادها و سازوکارهایی منجر به برخی افشای قابلیت‌های کلیدی و گزارش هک و نشت در چنین نهادهایی شده است. گزارش شده است که ایران همچنین بر روی جمع‌آوری اطلاعات دیجیتالی از طریق بازوهای نیابتی خود در مناطق مختلف درگیری کار کرده است که احتمالاً یکی از این مناطق عرصه جنگ داخلی سوریه بوده است (Scott-Railton, 2016). همچنین، حملات اسرائیل به گروه‌های سایبری حماس نشان‌دهنده تلاقی بین مبارزات آفلاین و آنلاین بین دو دشمن در سراسر سوریه و لبنان است (Chesney, 2019).

۲.۴ پاسخ‌های منطقه‌ای و بین‌المللی

این بخش از پاسخ‌های ملی و دوجانبه فوق به‌منظور در نظر گرفتن تحولات امنیت سایبری که منطقه خاورمیانه را به سایر مناطق و فرآیندهای بین‌المللی متصل می‌کند، حرکت کرده است. در گام اول، چندین طرح توسعه ظرفیت‌های امنیت سایبری فراملی با محوریت خاورمیانه وجود دارد (Kshetri, 2016). یکی از اولین تلاش‌ها، پیشنهاد ایجاد یک مرکز نظارتی پان عربی در سال ۲۰۰۹ بود که در لبنان مستقر باشد و اعضای همه کشورهای عربی را پوشش می‌داد. این پیشنهاد شامل چند وزارتخانه لبنان (کشور و دادگستری) و همچنین انجمن‌ها و دانشگاه‌های فناوری اطلاعات (IT) در لبنان و اتحادیه کشورهای عربی بود. این ایده اولیه چند سال بعد، در مارس ۲۰۲۰، با راه‌اندازی دستورالعمل‌های امنیت زیرساخت اینترنت برای کشورهای عربی توسط انجمن اینترنتی، یک سازمان غیرانتفاعی فراملی با اعضاء دولتی و شرکت‌ها، به ثمر رسید (Internet Society, 2020). این ابتکار، از جمله یک مرکز نظارتی جدید، نشان می‌دهد که فرآیندهای چندجانبه در منطقه خاورمیانه مفید هستند، زیرا گام‌های عملی را برای سازمان‌ها در مسیر ایمن‌سازی مکانیسم‌های مسیریابی و بهبود شیوه‌های امنیت سایبری ارائه می‌دهند. بدین اعتبار، کشورهای خاورمیانه در فرایندهای بین‌المللی حاکمیت امنیت سایبری از جمله (GGE[10]) و (OEWG[11]) در سازمان ملل شرکت کرده‌اند.

این فرایندهای بین‌المللی وسیع‌تر از مذاکرات گسترده بین‌المللی درباره جرائم سایبری است. اصلی‌ترین متن حقوقی بین‌المللی درباره جرائم سایبری، کنوانسیون بوداپست در مورد جرائم سایبری است که توسط شورای اروپا در سال ۲۰۰۱ به توافق رسید. به دنبال کنوانسیون بوداپست که دارای ۶۶ عضو پیوسته و ناظر است و تنها چهار دولت در منطقه خاورمیانه (ترکیه، اسرائیل، مراکش و تونس که عضو ناظر است) حضور دارند. به‌موازات این روند، اتحادیه کشورهای عربی کنوانسیون مبارزه با تخلفات فناوری اطلاعات را پیشنهاد داد. این کنوانسیون ابتدا در سال ۲۰۰۴ به‌عنوان قانون الگوی پان عربی برای مبارزه با تخلفات فناوری

[10] Group of Governmental Experts
[11] Open Ended Working Group

اطلاعات تصور شد و سرانجام در دسامبر ۲۰۱۰ امضا شد. این کنوانسیون عربی و رویدادهای هم‌زمان بهار عربی منجر به توسعه قوانین بحث‌انگیز جرائم سایبری شد و در سرتاسر منطقه، بسیاری از آن‌ها به‌عنوان بندهای مبهم مورد استفاده برای سرکوب انتقادها تعبیر شدند (Shires, n.d.). مذاکرات بین‌المللی فعلی در سازمان ملل متحد در حال بازبینی ایده یک معاهده جهانی جرائم سایبری است. با قطعنامه سال ۲۰۱۹ روسیه که به‌سرعت تقریبا از سوی همه دولت‌های خاورمیانه تأیید شد، اما تأثیر این مذاکرات بر قوانین داخلی تا چند سال ظاهر نخواهد شد. در مقایسه با جرائم سایبری، یک حوزه مذاکره‌کننده به همان اندازه کاربرد قوانین بین‌المللی درگیری‌های مسلحانه در عملیات سایبری از یک‌سو و اجرای دقیق‌تر هنجارهای رفتار مسئولانه دولت در فضای مجازی از سوی دیگر است که در GGE در سال ۲۰۱۵ و متعاقباً در چندین فرایند چندجانبه هر چند با نمایندگی محدود از منطقه مورد توافق قرار گرفت. چنین هنجارهایی شامل حفاظت از زیرساخت‌های حیاتی است که به‌وضوح توسط برخی از عملیات دولتی نقض شده و همچنین حفاظت از عرصه عمومی اینترنت نیز رعایت نشده است (Broeders, 2020). سایر ابتکارات مرتبط، مانند اقدامات ایجاد اعتماد (CBM[12]) برای کاهش خطر تشدید عملیات سایبری، به‌تازگی در حال پیشرفت در منطقه خاورمیانه است. به‌طور عملی، گنجاندن نهادهای فنی مانند گروه‌های واکنش اضطراری رایانه‌ای (CERTs[13]) در مکانیسم‌های تبادل اطلاعات و گفتگوی بین‌المللی، عملاً به ارائه کانال‌های ارتباطی می‌پردازند که ممکن است در سناریوهای بحرانی مفید باشد (Tanczer, 2018).

۵ نتیجه‌گیری

واقع‌گرایی به‌عنوان نظریه‌ای که بیشتر به مسائل امنیت ملی و قدرت مربوط می‌شود، به نظر می‌رسد دیدگاه غریزی روابط بین‌الملل برای درک فضای سایبری باشد. تحلیل مقاله به ما نشان داد که واقع‌گرایی یک چارچوب مرتبط برای شناسایی مسائل مهم مرتبط با امنیت در حوزه سایبری باقی می‌ماند و گاهی اوقات می‌تواند بینش مفیدی در مورد برخی از ویژگی‌های پایدار روابط بین‌الملل ارائه دهد. از بسیاری جهات، حوزه سایبری با ماهیت آنارشیک و فقدان حکومت نهادی، به دنیایی واقع‌گرا شباهت دارد که در آن دولت‌ها از یکدیگر می‌ترسند و توانایی‌های خود را در پاسخ به آن توسعه می‌دهند. بااین‌حال، مشخص نیست که آیا رقابت‌های تسلیحاتی سایبری احتمالاً به درگیری سایبری تبدیل می‌شود یا خیر. واقع‌گرایی همچنین سوالات جالبی را در مورد توان سایبری، در مورد اینکه چه کسی آن را در اختیار دارد و چگونه با ثبات منطقه‌ای و بین‌المللی مرتبط است، مطرح می‌کند. از نظر اینکه آیا توان سایبری پویایی قدرت سنتی را تغییر می‌دهد، شواهد نشان می‌دهد که این‌طور نیست. روندی که تاکنون دیده‌ایم از جنگ سایبری تمام‌عیار به نفع اشکال کمتر مخرب تعاملات و نیز همکاری‌های سایبری خودداری شده است.

با توجه به امکان‌پذیری در مورد استفاده از فناوری سایبری به‌عنوان یک سلاح تهاجمی، دولت‌های منطقه باید با احتیاط در حوزه سایبری عمل کنند و بر ایجاد دفاع انعطاف‌پذیر تمرکز کنند. در واقع، با خودداری از

[12] Confidence-Building Measures
[13] Computer Emergency Response Teams

جنگ سایبری آشکار، بسیاری از دولت‌ها تاکنون نسبتاً محتاطانه رفتار خود را در فضای سایبری حفظ کرده‌اند و این نتیجه‌ای است که نظریه‌پردازان واقع‌گرا آن را جذاب می‌دانند و زمینه‌ای برای تشریح نظری بیشتر است. با تحقیقات تجربی بیشتر، می‌توانیم به درک دقیق‌تری از مسائل کلیدی مانند تأثیر رقابت‌های تسلیحاتی سایبری بر روابط بین دولت‌های منطقه خاورمیانه، توزیع قابلیت‌های سایبری بین بازیگران دولتی و غیردولتی و دلایل خویشتن‌داری با وجود رقابت شدید امنیتی و تصور مزیت تهاجمی دست یابیم. پاسخ‌های دقیق‌تر به این سؤالات می‌تواند به ما در تدوین راهنمایی‌های بهتر سیاست‌گذارانه برای دولت‌ها و نیز سازمان‌های بین دولتی کمک کند.

دولت‌های خاورمیانه به‌شدت از چشم‌انداز تهدید جدید مرتبط با دیجیتالی شدن آگاه هستند. بسیاری از آن‌ها برای تقویت قابلیت‌های امنیت سایبری ملی خود و ارتقای سطح حفاظت از زیرساخت‌های اطلاعاتی مهم ملی خود، فعالیت‌های امنیت سایبری خود را در سال‌های اخیر افزایش داده‌اند. دولت‌های خاورمیانه تنها ذینفعانی هستند که از قدرت، دسترسی و منابع لازم برای توسعه و هدایت یک دستور کار واقعا ملی امنیت سایبری، اطمینان از همسویی تلاش‌ها و پیشبرد همکاری و بهبود مستمر از طریق بخش‌های خاص، ملی و در نهایت نهادهای حاکمیت منطقه‌ای برخوردار هستند. به همین دلیل است که دولت باید یک برنامه ملی امنیت سایبری را تعریف کند و مسئولیت آن را در بالاترین سطح تصمیم‌گیری تعیین کند. در پایان، چهار توصیه در عرصه سیاست‌گذاری دولتی را بر اساس مباحث فوق ارائه داده و با تأمل بر درک مضاعف ناامنی سایبری در پی پیاده‌سازی این موارد بر آمد:

- اول: دولت، بخش خصوصی و نهادهای جامعه مدنی باید برای افزایش تاب‌آوری سایبری همکاری کنند. آن‌ها باید با هم نقاط قوت و ضعف نسبی هر یک از ذینفعان را شناسایی کرده و به دنبال جبران این نقاط ضعف از طریق نقاط قوت مختلف باشند.

- دوم: دولت‌ها باید آموزش‌وپرورش را به‌عنوان پایه‌ای برای امنیت سایبری ملی و منطقه‌ای توسعه دهند. ابتکارات آموزشی باید در سراسر منطقه هماهنگ شده و برابری جنسیتی و بین بخشی را در اولویت قرار دهند.

- سوم: دولت‌ها باید بر اعتبار و قابلیت اطمینان بلندمدت در اقدامات و ارتباطات امنیت سایبری سرمایه‌گذاری کنند. این به معنای تدوین سیاست و مقررات مربوط به امنیت سایبری است که هم از نظر ماهیت و هم از نظر کاربرد قابل دسترسی باشد و به‌طور مداوم تفسیر و اجرا شود.

- چهارم: دولت‌ها باید در سطح بین‌المللی برای بالا بردن سطح امنیت سایبری در منطقه تلاش کنند. دولت‌ها می‌توانند از مفاهیم رفتار مسئولانه دولتی مسئول و عرصه عمومی اینترنت به‌عنوان مبنایی برای سرمایه‌گذاری در فرایندهای وسیع‌تر بین‌المللی مدیریت امنیت سایبری، توسعه حقوق بین‌الملل و مشارکت در گروه‌های کاری مرتبط در سازمان ملل استفاده کنند.

- در نهایت، این مقاله بر حس دوگانه ناامنی سایبری رایج در منطقه سایبری تاکید کرده است. ناامنی‌های سایبری، اعم از سطح بازیگران و نیز سطح ساختاری، خطرات روشنی را برای عملکردهای

اصلی دولت به همراه دارد: ثبات اقتصادهای دیجیتالی، عملکرد روان زیرساخت‌های حیاتی ملی و فراملی و حفاظت از افراد آسیب‌پذیر به‌صورت آنلاین و آفلاین.

اما ناامنی‌های سایبری همچنین در ناامنی‌های سیاسی وسیع‌تری گنجانده شده است، به‌ویژه در دولت‌ها و گستره‌هایی که حاکمان فعلی درگیر جنگ‌های منطقه‌ای و بین‌المللی هستند یا صداهای مخالف داخلی را برای جلوگیری از اعتراضات مردمی مسدود می‌کنند. به‌این‌ترتیب، ناامنی‌های سایبری – هم نفوذ به شبکه‌های دیجیتالی و هم دست‌کاری بسترهای رسانه‌های اجتماعی – تهدیدی برای قدرت سیاسی داخلی و منطقه‌ای و همچنین عملکردهای دولتی در راهبرد کلان است. در نتیجه، برخی دولت‌ها نه با هدف بهبود امنیت سایبری برای شهروندان و سازمان‌های تجاری در منطقه، بلکه برای حفظ موقعیت و موقعیت نخبگان همسو سرمایه‌گذاری کرده‌اند، درحالی‌که موقعیت مخالفان خود را کاهش داده یا بی‌ثبات می‌کنند. با دیجیتالی شدن منطقه خاورمیانه، افزایش جمعیت جوان و سرعت در حال رشد درصد کاربران آنلاین، ناامنی‌های سایبری نه‌تنها به ناامنی سیاسی تبدیل می‌شود، بلکه به‌طور فزاینده‌ای رسانه اصلی مشارکت سیاسی، اعتراض و رقابت بر سر روندهای آینده خواهد بود.

مراجع

[1] Ali, R. A., 2016. Cloud Computing in Arab States: Legal Aspect, Facts and Horizons, s.l.: ITU Arab Regional Office.

[2] Anderson, C., 2018. Iran's Cyber Threat: Espionage, Sabotage, and Revenge, s.l.: Carnegie Endowment for International Peace.

[3] Baezner, M., 2017. The Use of Cybertools in an Internationalized Civil War Context: Cyber Activities in the Syrian Conflict, Zurich: Center for Security Studies.

[4] Bain & Company and Google, 2019. E-Commerce in MENA: Opportunity beyond the Hype, s.l.: s.n.

[5] Broeders, D., 2020. Governing Cyberspace: Behavior, Power and Diplomacy, Lanham: Rowman & Littlefield.

[6] Cyber resilience in the GCC , 2021, Chatham House, https://www.chathamhouse.org/events/all/members-event/cyber-resilience-gcc.

[7] Chesney, R., 2019. Crossing a Cyber Rubicon? Overreactions to the IDF's Strike on the Hamas Cyber Facility, s.l.: Lawfare.

[8] Craig, A. & Valeriano, B., 2018. Realism and Cyber Conflict: Security in the Digital Age, s.l.: E-International Relations Publishing.

[9] DeSombre, W., 2021. Countering Cyber Proliferation: Zeroing in on Access-as-a-Service, Washington D.C: Atlantic Council Cyber Statecraft Initiative.

[10] Fakro, E., 2020. What the Abraham Accords Reveal About the United Arab Emirates, s.l.: War on the Rocks.

[11] Grossman, S., 2020. Blurring the Lines of Media Authenticity: Prigozhin-Linked Group Funding Libyan Broadcast Media, s.l.: The Stanford Internet Observatory Cyber Policy Center.

[12] Hakmeh,, J., 2020. Is the GCC Cyber Resilient?, London: Chatham House Royal Institute for International Affairs.

[13] Harknett, R., 2020. Troubled Vision: Understanding Recent Israeli-Iranian Offensive Cyber Exchanges, Washington D.C: Atlantic Council.

[14] Internet Society, 2020. Internet Infrastructure Security Guidelines for the Arab State, s.l.: s.n.

[15] ITU, 2018. Global Cybersecurity Index (GCI), s.l.: ITU Publications.

[16] Kantrowitz, A., 2020. How Saudi Arabia Infiltrated Twitter. [Online] Available at: https://www.buzzfeednews.com/article/alexkantrowitz/how-saudi-arabia-infiltrated-twitter.

[17] Kello, L., 2013. The Meaning of the Cyber Revolution Perils to Theory and Statecraft. International Security, 38(2), pp. 7-40.

[18] Kshetri, N., 2016. Cybersecurity in the Gulf Cooperation Council Economies. New York: Springer.

[19] Markets and Markets, 2020. Middle East Cybersecurity Market Worth $29.9 Billion by 2025, s.l.: PRNewswire.

[20] Möller, D., 2016. Guide to Computing Fundamentals in Cyber-Physical Systems—Concepts, Design Methods, and Applications. s.l.: Springer.

[21] Raymond, M., 2015. Multistakeholderism: Anatomy of an Inchoate Global Institution. International Theory, 7(3), p. 572–616.

[22] Scott-Railton, J., 2016. Group5: Syria and the Iranian Connection, s.l.: Citizen Lab.

[23] Shetty, S., 2018. Gartner Says Middle East and North Africa Enterprise Information Security Spending Will Grow 9.8 Percent in 2019, s.l.: Gartner.

[24] Shires, J., n.d. Ambiguity and Appropriation: Cybercrime in Egypt and the Gulf, London: Rowman & Littlefield Publishers.

[25] Sun, K., 2017. BankBot Seen on Google Play, Targets New UAE Bank Apps, s.l.: Trend Micro.

[26] Tanczer, L. M., 2018. CSIRTs and Global Cybersecurity: How Technical Experts Support Science Diplomacy. Global Policy, 9(3), pp. 60-66.

[27] Timberg, C., 2021. When U.S. Blamed Saudi Crown Prince for Role in Khashoggi Killing, s.l.: Washington Post.

[28] Unver, A., 2018. The Logic of Secrecy: Digital Surveillance in Turkey and Russia. Turkish Policy Quarterly, 17(2).