Applied Politics, Institute for Humanities and Cultural Studies (IHCS)
Biannual Journal, Vol. 4, No. 2, Autumn and Winter 2022-2023, 49-76

Cyber Threats in The Middle East Region and The Behavior of States

Seyed Hamed Hosseini*

Abstract

Cyber threats are a global phenomenon that is becoming increasingly complex and influential despite advances in technology and cybersecurity performance. Cybersecurity issues depend on a variety of factors: the growing reliance on information technology for various functions, the behavioral characteristics of political actors that lead to conflict and war, and the vulnerabilities of information technology that disrupt performance. This article addresses this fundamental question: Given the main sources of cyber insecurity in the region, how have states responded to this challenge? Relying on a realistic approach and a descriptive-analytical approach, this paper seeks to confirm the hypothesis that regional governments, as key players, have responded differently to cyber insecurity. At the national level, some states have sought to increase cybersecurity capacity, prioritizing important institutional and administrative changes such as digital defense and integration into military capabilities. At the international level, some countries in the region have also participated in negotiations on international cyber norms, while others in the region are outside the process. The results of this paper are based on several recommendations at the national policy level and also on cyber changes in the region.

Keywords: Cyber Security, Realism, Middle East, Threat, State.

* Ph.D. Candidate of Political Science, Gilan University, hamedhoseini@ut.ac.ir
Date received: 16/11/2022, Date of acceptance: 20/05/2023

سیاست کاربردی، پژوهشگاه علوم انسانی و مطالعات فرهنگی
دوفصل‌نامهٔ علمی (مقالهٔ پژوهشی)، سال ۴، شمارهٔ ۲، پاییز و زمستان ۱۴۰۱

تهدیدات سایبری در منطقهٔ خاورمیانه و رفتار دولت‌ها

سید حامد حسینی*

چکیده

تهدیدات سایبری یک پدیده 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 سوال اساسی پرداخته می‌شود: با توجه به منابع اصلی ناامنی سایبری در منطقه دولت‌ها چگونه به این چالش پاسخ داده‌اند؟ این نوشتار با تکیه بر رویکرد واقع‌گرایی و روش توصیفی-تحلیلی به دنبال تایید 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.

کلیدواژه‌ها: امنیت سایبری، واقع‌گرایی، خاورمیانه، تهدید، دولت.

* دانشجوی دکترای علوم سیاسی، دانشگاه گیلان، hamedhoseini@ut.ac.ir
تاریخ دریافت: ۱۴۰۱/۰۸/۲۵، تاریخ پذیرش: ۱۴۰۲/۰۲/۳۰

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 اساسا زندگی مردم را تغییر داده است. آن‌ها همچنین شیوه تجارت سازمان‌ها و نحوه ارائه خدمات دولتی و تعامل با شهروندان را تغییر می‌دهند. در عین حال، 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 به عنوان محیطی برای تعامل دولت ها، پیامدهای عمیقی برای امنیت بین‌المللی ایجاد کرده است. از یک‌سو، فضای سایبری فرصت‌هایی را برای کشورها فراهم کرده است تا در زمینه همکاری های نظامی و اطلاعاتی همکاری مؤثرتری داشته باشند. از سوی دیگر، رواج فضای سایبری باعث ایجاد تهدیدات منحصر به فردی شده است که نیازمند پاسخ‌های مستقیم سیاست‌گذارانه از سوی تصمیم‌گیرندگان است. درحالی‌که این فعل و انفعالات 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 بین رشته‌ای 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 به شدت در هم تنیده 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 زمینه های مختلف اجتماعی، ملی و منطقه‌ای متفاوت ظاهر می شوند؛ بنابراین امنیت سایبری از جمله در خاورمیانه و شمال آفریقا (MENA: the Middle East and North Africa) 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 به عنوان 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 به عنوان 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. با این وجود، 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. 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 به نوبه خود به پاسخ‌های بین‌المللی نیز می‌پردازد. این مقاله با چندین توصیه در عرصه سیاست‌گذاری براساس تغییرات اخیر در همسویی سیاسی در منطقه به پایان می‌رسد.

۱.۱ پیشینهٔ پژوهش

کتاب «امنیت سایبری بین‌المللی، انیکن تیک و میکا کرتونن، راتلج، ۲۰۲۰» در این موضوع به نگارش در آمده است. کتاب امنیت سایبری بین‌المللی توسعه و استفاده از فناوری اطلاعات و ارتباطات (ICT) را از منظر صلح و امنیت بین‌المللی بررسی می‌کند. با اذعان به اینکه مفهوم صلح و امنیت پیچیده تر شده است، این اثر به دنبال این است که مشخص کند کدام سؤالات امنیت سایبری واقعاً برای صلح و امنیت بین‌المللی مرتبط هستند و در عین حال که نیاز به توجه بین‌المللی دارند، مسائل مربوط به حکومت یا توسعه معاصر نیز هستند. این پژوهش، دیدگاه‌های موضوعی، منطقه‌ای و رشته‌ای متنوعی را در مورد مسئله امنیت سایبری بین‌المللی ارائه می‌کند و فصل‌های آن امنیت سایبری را در رقابت گسترده‌تر بر سر نظم جهانی، حقوق بین‌الملل، درگیری، حقوق بشر، حکومت‌داری و توسعه، زمینه‌سازی می‌کنند. این کتاب به چهار بخش موضوعی تقسیم شده است: مفاهیم و چارچوب‌ها؛ چالش‌های فضای سایبری امن و

صلح‌آمیز؛ دیدگاه‌های ملی و منطقه‌ای در مورد امنیت سایبری و در نهایت رویکردهای جهانی به امنیت سایبری. این کتاب برای دانشجویان امنیت سایبری، علوم کامپیوتر، جامعه‌شناسی، حقوق بین‌الملل، مطالعات دفاعی و به طور کلی روابط بین‌الملل بسیار مورد توجه خواهد بود.

کتاب «جنگ سایبری: یک تحلیل چند رشته‌ای، جیمز گرین، راتلج، ۲۰۱۵» نیز قابل توجه است. جنگ سایبری، به معنای تهاجم سایبری بین‌دولتی، یک پدیده نوظهور مهم و فزاینده در روابط بین‌الملل است، با حملات شبکه کامپیوتری سازمان‌دهی شده (ظاهراً سازمان‌دهی شده دولتی) در استونی (۲۰۰۷)، گرجستان (۲۰۰۸) و ایران (۲۰۱۰). این روش جنگ – با توجه به پتانسیل آن برای مثلاً سقوط هواپیماها از آسمان یا آسیب جدی نیروگاه‌های هسته‌ای ظرفیت آن را دارد که به اندازه هر وسیله متعارف برای انجام درگیری مسلحانه ویرانگر باشد. اکنون هر دولت در جهان یک برنامه دفاع سایبری دارد و بیش از ۱۲۰ دولت نیز برنامه حمله سایبری دارند. در حالی‌که میزان ادبیات جنگ سایبری در رشته‌ها در حال افزایش است، درک ما از این موضوع به دلیل عدم تعامل بین رشته ای محدود شده است. در پاسخ، این کتاب که برگرفته از حوزه‌های علوم کامپیوتر، استراتژی نظامی، حقوق بین‌الملل، علوم سیاسی و اخلاق نظامی است، بررسی انتقادی جنگ سایبری برای کسانی که از هر زاویه‌ای به این موضوع می‌پردازند، ارائه می‌کند. فصول کتاب به ظهور پدیده‌های جنگ سایبری در امور بین‌الملل می‌پردازد. حملات سایبری از منظر فناوری چیست؟ تا چه حد می توان حملات سایبری را به بازیگران دولتی نسبت داد. ارزش استراتژیک و خطر ناشی از درگیری سایبری چگونه است؛ مقررات قانونی حملات سایبری، هم به عنوان استفاده بین المللی از زور و هم به عنوان بخشی از یک درگیری مسلحانه جاری به چه ترتیب است و در نهایت پیامدهای اخلاقی جنگ سایبری مشتمل بر چه مواردی هست.

کتاب « امنیت سایبری در زیرساخت‌های حیاتی، استفن راب و دیگران، اشپرینگر، ۲۰۲۰» هم به این موضوع می پردازد؛ این کتاب مجموعه‌ای از مدل‌های تئوری بازی و تصمیم‌گیری را برای دستیابی و ارزیابی امنیت زیرساخت‌های حیاتی ارائه می‌کند. با توجه به گزارش‌های معاصر در مورد حوادث امنیتی از انواع مختلف، می توانیم شاهد تغییر الگو به سمت حملاتی با ماهیت ناهمگن باشیم که تکنیک‌های مختلف را در آنچه به عنوان یک تهدید پایدار پیشرفته می شناسیم ترکیب می کند. اقدامات احتیاطی امنیتی باید با این الگوهای تهدید متنوع به همان اندازه متفاوت باشد. در پاسخ، این کتاب تعداد زیادی تکنیک برای محافظت و کاهش ارائه می‌دهد. بسیاری از تحقیقات امنیتی سنتی تمرکز محدودی بر سناریوها یا برنامه‌های حمله

خاص دارند و تلاش می‌کنند تا حمله را عملا غیرممکن کنند. رویکرد جدیدتر به امنیت، آن را سناریویی می‌بیند که در آن هزینه یک حمله از پاداش بالقوه بیشتر است. این امر احتمال حمله را رد نمی‌کند، اما احتمال آن را تا کمترین خطر ممکن به حداقل می‌رساند. این کتاب این تعریف اقتصادی از امنیت را دنبال می‌کند و دیدگاه علمی مدیریتی را ارائه می‌کند که به دنبال تعادل بین سرمایه‌گذاری‌های امنیتی و مزایای ناشی از آن است و بر بهینه‌سازی منابع در پرتو تهدیداتی مانند تروریسم و تهدیدات پایدار پیشرفته تمرکز دارد. این کتاب با تکیه بر تجربه نویسندگان و با الهام از مطالعات موردی واقعی، رویکردی سامانمند به امنیت زیرساخت های حیاتی و انعطاف‌پذیری ارائه می‌دهد. این اثر با ارائه ترکیبی از کار نظری و داستان‌های موفقیت عملی، عمدتاً برای دانش‌پژوهان و تمرین‌کنندگانی است که به دنبال مقدمه‌ای بر تکنیک‌های نظری بازی و تصمیم گیری برای امنیت هستند. مفاهیم ریاضی مورد نیاز به صورت مستقل، با دقت معرفی شده و با مطالعات موردی نشان داده شده است. این تحقیق همچنین ابزارهای نرم‌افزاری را ارائه می‌دهد که به خوانندگان در استفاده عملی از مدل‌های علمی و چارچوب‌های محاسباتی کمک می‌کند.

کتاب « سیاست و فناوری فضای سایبری، دنی استید، راتلج، ۲۰۱۹» با پرداختن به مشکلات پیرامون امنیت سایبری و فضای سایبری، شکاف بین دنیای فنی و سیاسی را پر می‌کند تا درک ما از این نگرانی عمده امنیتی در جامعه وابسته به فناوری اطلاعات ما و خطرات ناشی از آن را افزایش دهد. تنها با ایجاد یک درک فنی صحیح از آنچه ممکن است و چیزی که ممکن نیست، می‌توان یک بحث آگاهانه به درستی انجام داد و دیدگاه‌های سیاسی نسبت به فضای سایبری و به طور دقیق‌تر آینده امنیت سایبری را ترسیم و پیش‌بینی کرد. نگارنده اثر با ترکیب تحقیقات از دنیای فنی که فضای سایبری ایجاد می‌کند با دنیای سیاسی، به دنبال درک پیامدها و کاربردهای فضای سایبری است و شرایطی را که منجر به موقعیت های کنونی شده است، تحلیل می‌کند و توضیح می‌دهد که در آن جوامع وابسته به فناوری اطلاعات در برابر هک، تروریسم، جاسوسی و جنگ سایبری آسیب پذیر بوده و به طور مرتب قربانی آن می‌شوند. دو سؤال اساسی در سراسر کتاب در نظر گرفته شده است: چه شرایطی منجر به این وضعیت شده است؟ و چه راهکارهایی برای آینده فضای سایبری وجود دارد؟ در برخورد با این سؤالات، نویسنده همچنین موقعیت های سیاسی نوظهور و رقابتی را که برای تثبیت چشم‌انداز فضای سایبری پیشنهاد می‌شود، تحلیل می‌کند. این کار میان‌رشته‌ای برای محققان و دانشجویان مطالعات امنیتی، مطالعات اطلاعاتی، مطالعات استراتژیک و روابط بین الملل و

همچنین متخصصان امنیت سایبری که مسئول گزینه‌های سیاست‌گذارانه هستند، جذاب خواهد بود.

«ایجاد حس توانایی های سایبری برای کشورهای کوچک: مطالعه موردی آسیا–اقیانوسیه، فرانسیس دومینگو، راتلج، ۲۰۲۲» پتانسیل قابلیت‌های سایبری را برای کشورهای کوچک در آسیا و اقیانوسیه به مثابه یکی از فعال‌ترین مناطق در خصوص موضوعات سایبری بررسی می‌کند. مطالعات در مورد تضاد و استراتژی سایبری در دهه گذشته به طور قابل توجهی افزایش یافته است، اما بیشتر آن‌ها بر روی عملیات سایبری بازیگران مسلط و قدرتمند متمرکز شده‌اند. این کتاب از برجستگی دولت‌های قدرتمند فاصله می‌گیرد و پتانسیل قابلیت‌های سایبری را برای کشورهای کوچک در آسیا و اقیانوسیه بررسی می‌کند. این اثر در واقع یک توضیح سامانمند از این مسئله است که چرا برونئی، نیوزلند و سنگاپور علیرغم ارزش استراتژیک مبهم خود، قابلیت‌های سایبری را توسعه داده‌اند یا در حال توسعه هستند. این اثر استدلال می‌کند که توزیع قدرت در منطقه و فرهنگ استراتژیک تکنولوژی محور دو شرط ضروری هستند که بر توسعه قابلیت‌های سایبری در کشورهای کوچک تأثیر می‌گذارند. به دنبال این استدلال، کتاب از واقع‌گرایی نئوکلاسیک به عنوان چارچوبی نظری برای توضیح تعامل بین این دو شرط استفاده می‌کند. این کتاب همچنین سه هدف فرعی را دنبال می‌کند. ابتدا، هدف آن تعیین محدودیت‌ها و مشوق‌هایی است که بر استفاده از قابلیت‌های سایبری به عنوان ابزار سیاست خارجی تأثیر می‌گذارد. دوم، عملکرد این قابلیت‌های سایبری را برای کشورهای کوچک ارزیابی می‌کند. در نهایت، پیامدهای استفاده از قابلیت‌های سایبری به عنوان ابزار سیاست خارجی کشورهای کوچک را ارزیابی می‌کند. این پژوهش منبع ارزشمندی برای دانشگاهیان و تحلیلگران امنیتی خواهد بود که روی درگیری سایبری، استراتژی نظامی، کشورهای کوچک و به طور کلی روابط بین‌الملل کار می‌کنند.

ادبیات مطالعات سایبری در دهه های گذشته به طور قابل توجهی افزایش یافته است. با این حال، تحقیقات در مورد منازعه سایبری و موضوعات مرتبط بسیار خاص، متمایل به سیاست‌گذاری است و لزوماً به ایجاد یا آزمایش تئوری‌های جریان اصلی برای مطالعه روابط بین‌الملل کمک نمی‌کند. در ادبیاتی که می‌توان آن را علمی در نظر گرفت، بیشتر مطالعات بر روی بازیگران قدرتمند، به ویژه رقابت بین چین، ایالات متحده و روسیه متمرکز شده است. علیرغم مشارکت فعال سایر دولت‌ها در فضای سایبری، ارتباط دولت‌های خاورمیانه در چالش‌های سایبری تا حد زیادی نادیده گرفته شده است.

عمده پیشینه‌های پژوهشی دست‌کم در یک دهه اخیر حاکی از این امر بوده است که تاکنون تحقیق دانشگاهی مشخصی در ارتباط با بررسی مسائل امنیت سایبری در خاورمیانه در سطح مقالات داخلی نیز صورت نگرفته است که می‌تواند به دلیل نوین بودن این حوزه از تهدیدها باشد یا اینکه هنوز به مسئله‌ای نزد محققان داخلی تبدیل نشده است. همچنین بیشتر تحقیقات دانشگاهی خارج از کشور نیز ناظر به پژوهش‌های اروپا محور یا بعضا شرق آسیا بوده است و در کل نگاهی ضعیف به حوزه امنیت سایبری در منطقه خاورمیانه داشته‌اند که با توجه به افزایش میزان تهدیدات از غفلت از پژوهش نیز تا منطقی به نظر نمی‌رسد.

۲.۱ چهارچوب نظری: واقع‌گرایی

با گسترش فناوری های اطلاعات و ارتباطات (ICT)، امنیت سایبری هم به منبع اصلی نگرانی برای سیاست‌گذاران تبدیل شده و هم مورد توجه محققان روابط بین‌الملل قرار گرفته است. ناامنی سایبری طیفی از ضرر مالی برای کسب‌وکارها از طریق جرائم سایبری، سرقت داده‌های طبقه‌بندی‌شده دولتی یا هدف قرار دادن زیرساخت‌های حیاتی را شامل شده و چالش مهمی را برای امنیت اقتصادی و ملی کشورها در سطح جهان ایجاد می کند. اکنون فضای سایبری به عنوان پنجمین حوزه جنگ پس از زمین، دریا، هوا و فضا در نظر گرفته می‌شود (The Economist, 2010) و چارچوب‌های نظری می‌توانند به ما در درک این شکل نسبتا جدید درگیری کمک کنند.

واقع‌گرایی از دیرباز پارادایم مسلط در حوزه روابط بین‌الملل بوده و بر مجموعه‌ای از مفروضات کلی در مورد سیاست بین‌الملل استوار است: دولت‌ها مهم‌ترین بازیگرانی هستند که به‌عنوان واحدهای مستقل در یک سیستم بین‌المللی فاقد اقتدار متمرکز عمل می‌کنند و به طور منطقی به دنبال منافع شخصی خود برای تضمین قدرت و امنیت هستند (Schmidt, 2002). حوزه امنیت سایبری در حال ظهور، تجدید حیات دیدگاه‌های متاثر از واقع‌گرایان را با تمرکز بر امنیت و رقابت، توزیع قدرت، مزیت حمله بر دفاع، و مزایای استراتژی های بازدارندگی نشان می‌دهد و از این رو فرصتی برای ارزیابی نقش واقع‌گرایی در این بحث‌ها فراهم می‌کند و با تمرکز بر مسائل امنیتی و درگیری، به نظر می رسد واقع گرایی به عنوان یک نظریه طبیعی برای روشن کردن مسائل امنیتی سایبری ضروری است.

برخی واقع‌گرایی را چارچوبی مفید برای درک فضای سایبری می‌دانند و بیان می‌کنند: نظریه‌های واقع‌گرایانه بازدارندگی، مدیریت بحران و درگیری ممکن است برای درک اینکه آیا

فضای سایبری در حال تثبیت یا بی‌ثباتی است، اینکه آیا فناوری‌های سایبری منبع جدیدی برای درگیری یا صلح خواهند بود و اینکه آیا دولت ها در مسابقه تسلیحاتی سایبری شرکت خواهند کرد، استفاده شود (Reardon, 2012). همچنین از جهاتی، آنارشی بین‌الملل و اثرات آن فضای سایبری را به خوبی توصیف می‌کند. نظریه‌پردازان لیبرال روابط بین‌الملل استدلال می‌کنند که تأثیرات خطرناک آنارشی را می‌توان توسط نهادهای بین‌الملل که میانجیگری اختلافات بین دولتی و کاهش عدم اطمینان از طریق افزایش اطلاعات است، بهبود بخشید (Russett, 2001, p. 164). با این حال، حوزه سایبری فاقد حکمرانی نهادی جهانی است. سازمان های مربوطه شامل اتحادیه بین‌المللی مخابرات(ITU/ International Telecommunications Union) و شرکت اینترنتی برای نام‌ها و شماره‌های اختصاص‌یافته (ICANN/ Internet Corporation for Assigned Names and Numbers) هستند، اما وظایف و صلاحیت‌های آن‌ها به مدیریت تعارض گسترش نمی‌یابد.

گزارش‌های رسانه‌ای از مسابقه تسلیحاتی سایبری مکرر است (Gordon, 2015) و این افزایش نظامی شدن فضای سایبری از طریق ایجاد سازمان‌های نظامی جدید، تهیه پیش‌نویس دکترین های نظامی–سایبری، افزایش بودجه امنیت سایبری و استخدام جنگجویان سایبری مشهود است. علاوه بر این، شواهد تجربی نشان دهنده رابطه بین افزایش قابلیت های سایبری و درک متقابل تهدید و رقابت بین دولت‌ها در تعدادی از موارد خاص است. واقع‌گرایی می‌تواند به توضیح منشأ رفتار مسابقه تسلیحاتی سایبری به عنوان پاسخی به تهدید در دنیای آنارشیک کمک کند، اما در فضای سایبری تشخیص قابلیت‌ها بسیار سخت است. اولا تأیید سوءاستفاده‌های تهاجمی که دولت‌ها در اختیار دارند، بسیار سخت است، زیرا بنا به تعریف، این اقدامات ناشناخته هستند. علاوه بر این، سازمان‌های نظامی سایبری مانند فرماندهی سایبری ایالات متحده تمایل دارند نقش های تدافعی و تهاجمی داشته باشند و اگر گفته شود که بودجه یا کارکنان خود را افزایش می دهند، مشخص نیست که سرمایه گذاری تهاجمی یا تدافعی انجام می‌شود. این امر به عدم اطمینان و رقابت بین دولت‌ها دامن می‌زند زیرا آن‌ها به دنبال امنیت در فضای سایبری هستند.

برای برخی واقع‌گرایان، رقابت‌های تسلیحاتی احتمال جنگ را افزایش می‌دهد، اما برای برخی دیگر، افزایش قدرت نظامی ابزار ضروری برای بازدارندگی یک قدرت تجدیدنظرطلب است؛ بنابراین یک سوال حیاتی این است که آیا رقابت امنیتی به درگیری واقعی تبدیل خواهد شد یا خیر. نگرانی در اینجا این است که آیا مسابقات تسلیحاتی سایبری به نتیجه مشابهی منجر خواهد شد یا خیر. درگیری در فضای سایبری با توجه به عدم اطمینان در مورد آنچه یک اقدام

جنگی است و تعداد فزاینده بازیگران دولتی و غیر دولتی که بـه دنبـال قابلیـت هـای تهـاجمی هستند، به طور منحصر به فردی مستعد تشدید است (Lord, 2011). با این حال، سوابق تجربـی نشان می‌دهد که اگرچه درگیری‌های سایبری در حال افزایش است، اما این افـزایش بـه جـای اشکال مخرب‌تر جنگ سایبری، با تاکتیک‌های مخرب و جاسوسی در سطح پایین مرتبط است. علاوه بر این، داده‌ها نشان می‌دهند که مناقشات سایبری بسیار بعید اسـت کـه بـه حـوزه‌هـای فیزیکی جنگ سرایت کنند و این نشان مـی‌دهـد کـه بـه جـای تشـدید، رونـد غالـب، نـوعی خویشتن‌داری است (Valeriano, 2016). به نظر می‌رسد دولت‌ها به‌جای انجام پیش‌بینی‌های مدل مارپیچی واقع‌گرایانه، از تشدید جنگ اجتناب می‌کنند و به نظـر مـی‌رسـد کـه خویشـتن‌داری هنجار غالب است.

۲. امنیت سایبری

امنیت اینترنت به یک چالش بزرگ تبدیل شده است. تقریباً هر چیزی که مـی بینـیم، لمـس یـا استفاده می‌کنیم به اینترنت متصل است، از جمله تلفن‌های همراه، وسایل فناورانه، لوازم خانگی و حتی وسایل نقلیه نیمه خودکار. اینترنت درگاهی برای مشاغل، دولت هـا و سـایر موسسـات است که دسترسی از راه دور به اطلاعات نظامی، اسرار تجاری، سوابق پزشکی و داده‌های مالی را فراهم می‌کند و این پارادوکس پدیده اتصال است؛ هرچه سامانه‌هـای کـامپیوتری مـا بیشـتر متصل باشند، بیشتر در معرض حملات سایبری شامل تلاش برای سرقت داده‌ها، خراب شـدن نرم‌افزار، اختلال در عملیات و حتی آسیب فیزیکی به سخت‌افزار و زیرساخت‌های شبکه قـرار می‌گیرند. حوزه امنیت سایبری برای مقابله با چالش درک و محافظت در برابر چنـین حملاتـی وجود دارد (Wilson, 2021, p. 1).

تجزیه و تحلیل تأثیر تحولات دیجیتالی و با استفاده از فناوری‌هـای دیجیتـالی پیشـرفته بـا توجه به تغییرات ناشی از آن در سازمان‌های دولتی و خصوصی نیاز به یک مرور کلی در سطح پیچیده سامانه‌ها، دستگاه‌ها و شبکه‌های هوشمند و به هم پیوسته مربـوط بـه خـود را دارد کـه برای انجام کارهای مربوطه مورد استفاده قـرار مـی‌گیـرد؛ بنـابراین، ایـن تجزیـه و تحلیـل در سازمان های دولتی و خصوصی نیازمند تحقیقات گسترده فناورانه و جامعه شناسانه با توجه بـه تعامل فناوری‌های دیجیتالی پیشرفته و همچنین مسائل مربوط به امنیت سایبری آن‌ها است کـه از طریق حملات و تهدیدهای سایبری به یک خطر ذاتـی تبـدیل مـی شـود؛ بنـابراین، امنیـت سایبری به عنوان یک رشته مبتنی بر محاسبات مبتنی بر حضور دشـمنان و در نتیجـه حمـلات

آن‌ها سروکار دارد. در حوزه علوم رایانه، حوزه امنیت سایبری حوزه‌های زیادی را شامل می‌شود، از جمله امنیت داده‌ها، رمزنگاری، امنیت نرم‌افزار و سخت‌افزار، امنیت شبکه و سیستم، حریم خصوصی و بسیاری از حوزه‌های دیگر؛ بنابراین، امنیت سایبری در فضای سایبری برای دو بخش اساسی است: هم از داده‌ها و اطلاعات محرمانه محافظت می‌کند و هم امکان دفاع از آن‌ها را فراهم می‌کند. در درجه اول فضای سایبری یک نهاد مصنوعی است که توسط بیت‌ها تشکیل شده است. در این زمینه، حملات و تهدیدهای سایبری با استفاده از فناوری‌های دیجیتالی پیشرفته و با قابلیت‌های به هم پیوسته خود به واقعیتی مهم تبدیل می‌شوند؛ بنابراین، امنیت سایبری را می‌توان مجموعه‌ای از دانش با توجه به فناوری‌ها، فرایندها و شیوه‌هایی دانست که برای محافظت از سامانه‌ها، شبکه‌ها یا برنامه‌های رایانه‌ای و همچنین داده‌های فضای مجازی در برابر حمله، آسیب یا دسترسی غیر مجاز طراحی شده‌اند (Möller, 2016). در این رابطه عناصر امنیت سایبری شامل موارد زیر است:

الف– امنیت برنامه: اقدامات امنیتی در سطح برنامه برای ایمن‌تر کردن برنامه‌ها از طریق یافتن، رفع و ارتقای امنیت برنامه ها، برای جلوگیری از به خطر افتادن، خراب شدن، سرقت یا ربوده شدن داده‌ها یا کدهای درون برنامه انجام می‌شود. بیشتر این حملات در فاز توسعه اتفاق می‌افتد، اما شامل ابزارها و روش‌هایی برای ایمن‌سازی برنامه‌ها پس از استقرار آن‌ها می‌شود. این امر اهمیت بیشتری پیدا می‌کند زیرا هکرها به طور فزاینده برنامه‌ها را با حملات خود هدف قرار می‌دهند.

ب–امنیت رایانه: حفاظت از سامانه یا شبکه کامپیوتری در برابر آسیب، سرقت و استفاده غیرمجاز و همچنین اختلال یا هدایت نادرست خدمات ارائه شده توسط آن‌ها. این امر به دلیل افزایش وابستگی به سامانه‌های رایانه‌ای و رشد دستگاه‌های هوشمند اهمیت پیدا می‌کند. امنیت رایانه به چهار تهدید بزرگ سایبری اشاره دارد: کلاه‌برداری، تجاوز به حریم خصوصی مانند دسترسی غیرقانونی به داده‌های محافظت شده، سرقت اطلاعات و در نهایت خرابکاری یا نابودی داده‌ها توسط یک ویروس رایانه‌ای.

ج–امنیت داده‌ها: مجموعه‌ای از استانداردها و فناوری‌ها برای جلوگیری از دسترسی غیرمجاز به سامانه‌های رایانه‌ای، پایگاه داده‌ها و سایر موارد برای محافظت از داده‌ها در برابر تخریب عمدی یا تصادفی، خرابی داده‌ها، تغییر یا افشای آن‌ها. امنیت داده‌ها یک موضوع اساسی امنیت فناوری اطلاعات برای سازمان های دولتی و خصوصی است که از تکنیک ها و فن‌آوری‌هایی از جمله کنترل‌های اداری، امنیت فیزیکی، کنترل‌های پشتیبانی، استانداردهای

سازمانی و سایر تکنیک‌های حفاظتی برای به حداقل رساندن یا جلوگیری از دسترسی به کاربران یا فرآیندهای غیرمجاز یا مخرب حمایت می‌کند.

د–بازیابی آسیب‌ها و برنامه‌ریزی برای تداوم کسب و کار: شیوه‌های مشابه با هدف محدود کردن خطر تهدیدات سایبری و مجبور ساختن سازمان‌های دولتی و خصوصی به انجام وظایف تجاری خود تا حد ممکن به منظور بازگشت به حالت عادی پس از یک حادثه غیرمنتظره. با افزایش تهدیدات سایبری و کاهش تحمل زمان خرابی، بازیابی خسارات و برنامه‌ریزی به جهت تداوم کسب و کار اهمیت می‌یابد؛ بنابراین، یک روند مداوم برای ترکیب بازیابی حوادث و برنامه‌ریزی برای استمرار تجارت و کسب و کار مورد نظر است.

ه–امنیت اطلاعات: استراتژی طراحی شده برای محافظت از محرمانه بودن، یکپارچگی و در دسترس بودن داده‌های سامانه‌های رایانه‌ای یا بسته‌های شبکه در برابر کسانی که دارای نیت مخرب هستند. امنیت اطلاعات شامل مجموعه‌ای از استراتژی‌ها برای مدیریت فرایندها، ابزارها و سیاست های لازم برای جلوگیری، تشخیص، مستندسازی و مقابله با تهدیدات سایبری برای اطلاعات دیجیتالی و غیر دیجیتالی است؛ بنابراین، امنیت اطلاعات عملی است که از دسترسی غیرمجاز، تخریب، افشا، اختلال، بازرسی، اصلاح یا استفاده از اطلاعات غیرمجاز جلوگیری می‌کند.

و–امنیت شبکه: اصطلاحی که شامل بسیاری از فناوری‌ها، دستگاه‌ها و فرایندهای ایمن سازی شبکه‌ها می‌شود. این اصطلاح به مجموعه‌ای از قوانین و تنظیمات اشاره دارد که برای محافظت از محرمانه بودن، یکپارچگی و دسترسی سامانه‌ها یا شبکه‌های رایانه‌ای و همچنین داده‌ها با استفاده از فناوری‌های نرم‌افزاری و سخت‌افزاری طراحی شده است. معماری شبکه‌های نوین پیچیده است و با محیطی تهدیدآمیز که همیشه در حال تغییر است مواجه است و مهاجمان تهدید سایبری که همیشه در تلاش برای یافتن و بهره‌برداری از آسیب‌پذیری‌ها هستند. این آسیب‌پذیری‌ها می‌توانند در تعداد زیادی از مناطق از جمله دستگاه‌ها، داده‌ها، برنامه‌ها، کاربران و مکان‌ها وجود داشته باشند؛ بدین سبب، امنیت شبکه عملی است که از حوادث نفوذ به شبکه‌های عمومی و خصوصی شرکت و سازمان‌ها جلوگیری می‌کند و از آن محافظت می‌کند (Möller, 2020, pp. 4-6).

با این وجود، یکی از مشکل‌سازترین عوامل امنیت سایبری، ماهیت سریع و دائما در حال تحول خطرات حمله سایبری است. رویکرد سنتی این بوده است که بیشتر منابع بر مهم ترین فرایندها متمرکز شده و در برابر بزرگ‌ترین تهدیدهای شناخته شده محافظت می‌کند و برخی از

سامانه‌ها یا اجزای کم‌اهمیت بدون دفاع سامانه‌ها یا اجزای آن در معرض برخی خطرات کم‌اهمیت قرار می‌گیرند. چنین رویکردی دیگر برای سامانه‌های رایانه‌ای یا محیط‌های شبکه‌ای سازمان‌های پیچیده دولتی و خصوصی مبتنی بر فناوری پیشرفته دیجیتال کافی نیست. در این زمینه، متخصصان امنیت سایبری فرض می‌کنند که رویکردهای سنتی برای ایمن‌سازی سامانه‌های رایانه‌ای یا خصوصی اطلاعات شبکه‌ها می‌توانند غیرقابل مدیریت باشد زیرا محیط حمله سایبری به طرز غیرقابل قبولی پیچیده شده است، به طوری که بررسی ها و مداخلات دستی و نیمه‌خودکار امنیت سایبری نمی‌توانند دیگر سازگار باشند و به طور مداوم در حال تحول چشم‌اندازهای حملات و تهدیدهای سایبری هستیم. از این رو، سامانه‌ها یا شبکه‌های رایانه‌ای سازمان‌های دولتی و خصوصی به دلیل در دسترس بودن و ارتباط همه‌جانبه که در معرض حملات از راه دور قرار می گیرد، در برابر حملات سایبری آسیب پذیرتر شناخته شده‌اند. در این زمینه، گروه های امنیت سایبری در سراسر جهان در حال تلاش برای تجزیه و تحلیل آسیب‌پذیری‌ها هستند تا اطلاعات عمیق‌تری در مورد آن‌ها به دست آورند تا بر اساس استراتژی‌های کارآمد امنیت سایبری برای دفاع از حملات و تهدیدهای سایبری آمادگی لازم را در اختیار داشته باشند.

۳. اشتراک در ناامنی‌های سایبری

درک ناامنی های سایبری هم به عنوان یک تهدید دیجیتالی واقعی و هم به عنوان احساس عدم اطمینان سیاسی برای تجزیه و تحلیل امنیت سایبری در منطقه خاورمیانه بسیار مهم است (Hassib, 2021). اولین نوع ناامنی ناشی از نفوذ یا هک است که به عنوان توانایی دسترسی غیرمجاز به دستگاه ها و شبکه های دیجیتالی و استفاده از این دسترسی برای اهدافی برخلاف قصد صاحبان و طراحان آن‌ها تعریف می‌شود (Shires, 2019). این اهداف می‌تواند شامل پاک‌سازی داده‌ها (در موارد جاسوسی و نظارت سیاسی یا صنعتی)، تغییر یا حذف داده‌ها (مانند پاک کردن بدافزار یا باج افزار که داده‌های هدف را رمزگذاری می‌کند)، یا حتی آسیب یا تخریب فیزیکی (جایی که هدف شبکه‌ها سامانه‌های کنترل صنعتی یا زیرساخت‌های حیاتی هستند).

نوع دوم ناامنی ناشی از دست‌کاری شبکه‌های دیجیتال و در درجه اول بسترهای رسانه‌های اجتماعی است. در حال حاضر یک اجماع گسترده وجود دارد که می توان از بسترهای رسانه‌های اجتماعی برای کمپین‌های نفوذ که مواضع سیاسی یا سایر موضوعات را به روش‌های

نامشروع ارتقا می دهند، سوء استفاده کرد. به عنوان مثال بـا اسـتفاده از حسـاب هـای خودکـار (ربات‌ها)، با ایجاد عمدی ادعاهای نادرست و غیر قابل تأییـد (اطلاعـات غلـط)، یـا بـا سـوء استفاده از آسیب‌پذیری‌های روانی از طریق تبلیغات. هر دو مجموعه ناامنی می‌توانند با هـم رخ دهند، به عنوان مثال در عملیات هک و نشت، از نفوذ برای به دست آوردن مطالبی که بعداً بـه نفع سیاسی یا مهندسی اجتماعی منتشر می‌شود، استفاده می‌گردد که در آن دسترسی بـه شـبکه بدون سوء استفاده از آسیب‌پذیری‌های فنی مورد نظر است (Shires, 2019).

در حالی که این دو مجموعه از ناامنی ها هر دو ویژگی سامانه های فنی و اجتماعی هسـتند، اما بعد سیاسی موضوع، زیربنای بحث ناامنی سـایبری اسـت. بسـیاری از دولـت‌هـای منطقـه خاورمیانه دارای نظام‌های اقتدارگرا یا ترکیبی از نیمه سنتی و نیمه اقتدارگرا هستند کـه قـدرت سیاسی واقعی یک بدنه نخبه را پنهان می‌کنند. چنین دولت‌هایی نه تنها از نظر نفوذ، بلکه از نظر موقعیت رژیم فعلی نیز ناامن هستند. مجموعه اعتراضات مردمی معروف بـه بهـار عربـی ایـن ناامنی ها را به وضوح نشان داد و نشان داد که چگونه رسانه های اجتماعی (بـه عنـوان یکـی از عوامل) می توانند در تغییرات گسترده سیاسی و نتایج نهایی آن مانند گذار دموکراتیک، کـاهش قدرت استبدادی یا جنگ داخلی ویرانگر کمک کنند. در حالی که بسیاری از کشورها، از جمله کشورهای حوزه خلیج فارس و مصر، به پتانسیل سیاسی اقدامات سیاسی برخط پـس از بهـار عربی پی بردند، اما آن‌ها این نگرانی‌ها را با سایر مسائل مربوط به امنیت سایبری مرتبط نکردند، مگر پس از حوادث کلیدی مورد بررسی مانند حمله سایبری با یک باج افزار به شـرکت نفتـی آرامکو عربستان در سال ۲۰۱۲. در پی این حادثه کشورهای حوزه خلیج فارس سرمایه‌گـذاری گسترده‌ای در زمینه امنیت سایبری هم از طریق رویدادها و اجلاس‌های تجاری و هم آموزش و آگاهی داخلی انجام دادند (Shires, 2018).

۱.۳ منابع ناامنی سایبری مبتنی‌بر بازیگران منطقه

منابع امنیت سایبری مبتنی بر بازیگران در منطقـه خاورمیانـه را مـی تـوان در سـه نـوع اصـلی طبقه‌بندی کرد: رقابت و درگیری بین دولتی، زمینه‌های حملات و جنگ‌های داخلـی و جـرائم سایبری که به ترتیب توضیح داده خواهند شد. اول، منطقـه خاورمیانـه از وضـعیت جاسوسـی سایبری به عنوان ابزاری برای پیشبرد منافع منطقه‌ای مستثنا نیست. شرکت‌های امنیت سـایبری، کمپین های جاسوسی سایبری را با هدف قرار دادن نهادهای دولتی و خصوصی در تعـدادی از

کشورهای خاورمیانه و همچنین عملیات جاسوسی سایبری قدرتمند از سوی قدرت‌های بزرگ و فرامنطقه نسبت داده‌اند.

به عنوان نمونه، پس از افشای عملیات خرابکارانه موسوم به استاکس نت (Stuxnet) در سال ۲۰۱۰ علیه برنامه هسته‌ای ایران، عملیات سایبری مختل کننده دولتی به دلیل تنش‌ها در خلیج فارس شروع شد؛ از جمله عملیات علیه زیرساخت‌های حیاتی در عربستان از سال ۲۰۱۲ (از جمله 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 به ویژه 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 که مهم‌ترین آن‌ها ارتش الکترونیکی سوریه (SEA: Syrian Electronic Army) وابسته به حکومت اسد است (Baezner, 2017). اعضای ائتلاف بین‌المللی در سوریه ادعا کرده‌اند که عملیات سایبری علیه داعش(ISIS: the Islamic State of Iraq and Syria) ، 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). به طور 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. در حالی که 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. به عنوان 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. به عنوان مثال، باج‌خواهی به دنبال به اشتراک‌گذاری تصاویر خصوصی، جنبه مهم اما ناشناخته‌ای از امنیت سایبری در سطح شخصی و خانوادگی است تا عرصه دولتی.

۲.۳ 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 از جمله 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 G۵ و هوش مصنوعی(Artificial Intelligence/AI) برای این کشورها بسیار جذاب است؛ بدین لحاظ، آن ها به دنبال ایجاد تعادل بین همکاری اقتصادی چین و الزامات امنیتی ایالات متحده بوده‌اند (Hakmeh,, 2020).

تحولات ژئوپلیتیک از جهات دیگر بر امنیت سایبری خاورمیانه تأثیر می‌گذارد. به عنوان مثال، تقویت قوانین حفاظت از داده‌های اتحادیه اروپا از طریق مقررات عمومی حفاظت از داده‌ها (GDPR/ the General Data Protection Regulation) 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 (cloud computing) را در سراسر منطقه، به ویژه 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 پروژه های جدید شهری مانند Neom در 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 به ویژه 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 می شوند. کشورهایی مانند عربستان سعودی برای دور زدن این محدودیت ها از روش‌های غیرمتعارف استفاده کرده‌اند، مانند استخدام افراد داخلی در دفاتر توییتر در کالیفرنیا برای ارائه اطلاعات در مورد حساب‌های خاص (Kantrowitz, 2020). به طور گسترده‌تر، اکثر بازیگران منطقه‌ای بر معماری‌های نظارتی در سطح ملی، با حمایت از قوانین گسترده جرائم سایبری، برای نظارت بر رسانه های 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.

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 می توانیم پاسخ های دولت را به عنوان چندین هدف متمایز، از جمله بازدارندگی (منصرف کردن عوامل تهدیدکننده از هدف قرار دادن آن دولت)، دفاع (بهبود حفاظت و آگاهی از امنیت سایبری، به ویژه از طریق ظرفیت‌سازی) و تاب‌آوری (اطمینان از تداوم عملکردهای اصلی دولت با وجود اختلال سایبری) مورد نظر 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 ۲۰۲۰ انجام شد، عربستان سعودی، امارات و عمان در زمینه امنیت سایبری سه کشور برتر جهان عرب و در رتبه‌های بعدی قطر، بحرین و کویت قرار گرفتند (ITU, 2020). این دولت‌ها گام‌های مهمی در جهت ایمن‌سازی دیجیتالی خدمات دولتی برداشته‌اند و امارات متحده عربی از بسیاری جهات از سایر کشورها جلوتر است در حالی که سایر دولت‌های خاورمیانه نمرات ضعیف‌تری دارند. بر اساس مطالعه ۲۰۱۹ توسط Google و Bain & Company، بازار تجارت الکترونیک در سال ۲۰۱۷ در منطقه خاورمیانه به طور کلی ۸.۳ 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 به عنوان مرکز سایبری منطقه در نظر گرفته است؛ با توجه به اینکه این کشورها ۸۰ درصد از بازار تجارت الکترونیکی منطقه را به طور کلی (به استثنای 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 می دهد بازار امنیت سایبری خاورمیانه در سال ۲۰۲۰ بـه ارزش حـدودا ۱۶ میلیـارد 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 یک بار چنین استراتژی را منتشـر کـرده‌انـد و بسـیاری از آن‌ها چندین بار استراتژی‌های خود را به روز کرده‌اند. بسیاری از دولت‌های منطقه تلاش‌هـای گسترده‌ای را در زمینه آموزش امنیت سایبری با ارائه مدارک در زمینه‌های فنی و سازمانی انجام داده‌اند و همچنین راه‌های عملی‌تر برای نقش‌های حرفه‌ای امنیـت سـایبری و افـزایش آگـاهی عمومی را بر عهده گرفته‌اند. این دوره‌ها به ویژه توسط زنان پذیرفته شـده اسـت و جنبـه‌هـای جنسیتی هویت‌های حرفه‌ای و شخصی امنیت سایبری و عوامـل سـاختار بخـش قـوی بـرای ظرفیت‌سازی امنیت سایبری در منطقه خاورمیانه صورت پذیرفته است.

از نظر نهادی، برخی دولت‌های منطقه مسئولیت‌های امنیت سایبری را در یک سازمان ملـی امنیت سایبری متمرکز کرده‌اند. کشورهایی که در سال گذشته این کار را انجام داده‌اند عبارت‌اند از عمان، بحرین و قطر؛ در حالی که سایر کشورها چندین ترتیبات نهادی مانند شـورای عـالی امنیت سایبری مصر یا آژانس ملی امنیت الکترونیکی امارات (NESA) را تاسیس کرده اند. چنین سازمان‌هایی برای ادغام عملکردهای مجازی قبلی که در وزارتخانه‌هـای ارتباطـات و کشـور و غیره ادغام شده‌اند طراحی شده است. حساس‌تـرین جنبـه ایـن سیاسـت بوروکراتیـک، بـرای دولت‌های خاورمیانه و همتایان خود در ایالات متحده و اروپا، رابطه بین چنین سازمان‌هایی بـا سازمان‌های نظامی و اطلاعاتی است. ارزیابی‌ها نشان داده‌اند کـه چگونـه مـثلا در ترکیـه، ایـن رقابت نهادی منجر به نقش امنیتی غالب در چنین تحولاتی شده است، در حـالی کـه دیگـران پتانسیل چنین موسساتی را در فضاهای مورد مناقشـه ماننـد گسـتره فلسـطین و اسـرائیل نقـد کرده‌اند (Unver, 2018).

دولت‌های دیگر مانند تونس، شامل ترتیبات چند ذی‌نفع را که شامل بخـش‌هـای دولتـی و خصوصی و نمایندگان جامعه مدنی می‌شود، مطابق با ترتیبات گسترده‌تر چندجانبه در مدیریت جهانی اینترنت دنبال کرده‌اند. به طور کلی، به استثنای اسرائیل و ایران، سایر دولت‌های منطقه به دلیل عدم وجود ساختارهای سایبری نظامی عمومی و عدم ایجاد دستورات سـایبری جداگانـه، قابل توجه هستند. این ممکن است به دلیل عدم توانایی به طور کلی یا به این دلیـل باشـد کـه منبع قدرت سایبری در جای دیگری مانند سازمان‌های اطلاعـاتی قـرار دارد، یـا ایـن کـه ایـن

کشورها ترجیح می‌دهند با ایجاد برنامه‌های سایبری تهاجمی، سیگنال‌های جداگانه‌ای را ارسال نکنند (Raymond, 2015).

علاوه بر این، دولت‌ها مشارکت‌های دوجانبه جدید یا تقویت شده‌ای 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 ایجاد شده را آشکار می‌کند. نمونه این مشارکت در تولید امنیت سایبری مثالی بین امارات و عربستان است. اگرچه به طور 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 می تواند به ایجاد ارتباط در خطوط طولانی سایبری کمک کند. به عنوان 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). با این حال، 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، به ویژه حرکات اسرائیل، مقابله با موفقیت ایران در شیوه بسیار 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. در عین حال، ایران صحنه سایبری قابل توجهی را پرورش داده است، به طوری که 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 نشان دهنده 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 به منظور 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 می داد. این پیشنهاد شامل چند وزارتخانه لبنان (کشور و دادگستری) و همچنین انجمن ها و دانشگاه های 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/ Group of Governmental Experts) و (OEWG/ Open Ended Working Group) 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. به موازات این روند، اتحادیه کشورهای عربی کنوانسیون مبارزه با تخلفات فناوری اطلاعات را پیشنهاد داد. این کنوانسیون ابتدا در سال ۲۰۰۴ به عنوان قانون الگوی پان عربی برای مبارزه با تخلفات فناوری

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 به عنوان 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 به سرعت 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 یک سو 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 به وضوح 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/ confidence-building measures) برای کاهش خطر تشدید عملیات سایبری، به تازگی در حال پیشرفت در منطقه خاورمیانه است. به طور عملی، گنجاندن نهادهای فنی مانند گروه‌های واکنش اضطراری رایانه‌ای (CERTs/Computer Emergency Response Teams) 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 به عنوان 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 واقع گرایی 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. با این حال، 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.

استدلال مشخص مقاله این بود 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، در حالی که برخی دیگر مسئولیت و توانایی را بین سازمان‌های بین دولتی تقسیم کرده‌اند. به طور مشابه، در سطح بین‌المللی، برخی از دولت‌ها به طور گسترده در مذاکرات حکمرانی امنیت سایبری مشارکت داشته‌اند، در حالی که 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.

با توجه به عدم قطعیت در مورد استفاده از فناوری سایبری به عنوان 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 جنگ سایبری آشکار، بسیاری از دولت ها تاکنون نسبتاً محتاطانه رفتار خود را در فضای سایبری حفظ کرده‌اند و این نتیجه‌ای است که نظریه‌پردازان واقع‌گرا آن را جذاب می دانند و زمینه‌ای برای تشریح نظری بیشتر است. با تحقیقات تجربی بیشتر، می توانیم به درک دقیق تری از مسائل کلیدی مانند تأثیر رقابت های تسلیحاتی سایبری بر روابط بین دولت های منطقه خاورمیانه، توزیع قابلیت های 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 کمک کند.

دولت‌های خاورمیانه به شدت 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 تلاش ها و پیشبرد همکاری و بهبود مستمر از طریق بخش های 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 تاب آوری 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: دولت ها باید آموزش و پرورش را به عنوان پایه ای 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: دولت ها 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 به طور 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 به عنوان مبنایی برای سرمایه گذاری 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، به ویژه در دولت‌ها و مناطقی که حاکمان فعلی درگیر جنگ‌های داخلی بین‌المللی هستند یا صداهای مخالف را برای جلوگیری از اعتراضات مردمی مسدود می‌کنند. به این ترتیب، ناامنی‌های سایبری – هم نفوذ به شبکه‌های دیجیتالی و هم دست‌کاری بسترهای رسانه‌های اجتماعی – تهدیدی برای قدرت سیاسی داخلی و منطقه ای و همچنین عملکردهای دولتی در استراتژی کلان است. در نتیجه، دولت‌ها نه تنها با هدف بهبود امنیت سایبری برای افراد و سازمان‌های

تجاری در منطقه، بلکه برای حفظ موقعیت و موقعیت نخبگان سرمایه‌گذاری کرده‌اند، در حالی که موقعیت مخالفان خود را کاهش داده یا بی‌ثبات می‌کنند. با دیجیتالی شدن منطقه خاورمیانـه، با افزایش جمعیت جوان و سرعت در حال افزایش درصد کاربران آنلاین، ناامنی های سـایبری نه تنها به ناامنی سیاسی تبدیل می شود، بلکه به طور فزاینده‌ای رسانه اصلی مشارکت سیاسی و رقابت بر سر آینده خود خواهد بود.

کتاب‌نامه

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

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

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

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

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

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

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

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

Gordon, C., 2015. *Rapid escalation of the cyber-arms race*. [Online] Available at: http://www.bbc.co.uk/news/uk-32493516

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.

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

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

Hassib, B., 2021. Manipulating Uncertainty: Cybersecurity Politics in Egypt. *Journal of Cybersecurity*, 7(1).

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

ITU, 2020. *Global Cybersecurity Index (GCI)*, s.l.: ITU Publications.

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

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

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

Lord, K., 2011. *America's Cyber Future: Security and Prosperity in the Information Age*, s.l.: Center for a New American Security.

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

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

Möller, D., 2020. *Cybersecurity in Digital Transformation: Scope and Applications*. s.l.:Springer.

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

Reardon, R., 2012. *The Role of Cyberspace in International Relations: A View of the Literature*, San Diego: ISA Annual Convention.

Russett, B., 2001. *Triangulating Peace: Democracy, Interdependence, and International Organizations*. New York: Norton & Company.

Schmidt, B., 2002. On the History and Historiography of International Relations. In: W. Carlsnaes, ed. *Handbook of International Relations. London*: Sage Publications, pp. 3-22.

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

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

Shires, J., 2018. Enacting Expertise: Ritual and Risk in Cybersecurity. *Politics and Governance*, 6(2), pp. 31-40.

Shires, J., 2019. Family Resemblance or Family Argument? Three Perspectives of Cybersecurity and Their Interaction. *St Anthony's International Review*, 14(3), pp. 18-36.

Shires, J., 2019. Hack-and-Leak Operations: Intrusion and Influence in the Gulf. *Journal of Cyber Policy*, 4(2), pp. 233-56.

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

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

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

The Economist, 2010. *War in the fifth domain: Are the mouse and keyboard the new weapons of conflict?*. [Online] Available at: https://www.economist.com/briefing/2010/07/01/war-in-the-fifth-domain

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

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

Valeriano, B., 2016. *Cyber Spillover Conflicts: Transitions from Cyber Conflict to Conventional Foreign Policy Disputes?*. London: Routledge.

Wilson, D., 2021. *Cybersecurity*. Massachusetts: The MIT Press Essential Knowledge series.