عمق ژئوپلیتیک دیجیتال

(جلد ۱)

تألیف

دکتر افشین متقی دستنائی

استاد جغرافیای سیاسی دانشگاه خوارزمی

دکتر علی کرمی

دانشگاه خوارزمی

تهران ۱۴۰۳

سرشناسه	:	مقی‌دستایی، افشین، ۱۳۶۲-
عنوان و نام پدیدآور	:	عمق ژیوپلیتیک دیجیتال/تالیف افشین مقی‌دستائی، علی کرمی.
مشخصات نشر	:	تهران: دانشگاه خوارزمی ، ۱۴۰۳-
مشخصات ظاهری	:	۲ ج.
شابک	:	دوره ۵-۰۹-۴۸۱۵-۶۲۲-۹۷۸ ج. ۱. ۱-۱۰-۴۸۱۵-۶۲۲-۹۷۸ ج .۲. ۸-۱۱-۴۸۱۵-۶۲۲-۹۷۸
وضعیت فهرست نویسی	:	فیا
یادداشت	:	کتابنامه.
موضوع	:	سیاست جغرافیایی Geopolitics؛ فضای مجازی -- جنبه‌های سیاسی Cyberspace -- Political aspects؛ جغرافیای سیاسی Political geography
شناسه افزوده	:	کرمی، علی، ۱۳۶۲- دانشگاه خوارزمی
رده بندی کنگره	:	JC۳۱۹
رده بندی دیویی	:	۳۲۰.۱
شماره کتابشناسی ملی	:	۹۶۷۶۳۱
اطلاعات رکورد کتابشناسی	:	فیا

عنوان کتاب	:	**عمق ژئوپلیتیک دیجیتال** (جلد ۱)
تألیف	:	دکتر افشین مقی دستائی، دکتر علی کرمی
ناشر	:	دانشگاه خوارزمی
چاپ و صحافی	:	دانشگاه خوارزمی
صفحه‌آرا	:	مسعود سلیمانی
طراح جلد	:	مسعود سلیمانی
نوبت و سال چاپ	:	اول، ۱۴۰۳
شابک دوره	:	۵-۰۹-۴۸۱۵-۶۲۲-۹۷۸
شابک جلد اول	:	۱-۱۰-۴۸۱۵-۶۲۲-۹۷۸
شمار	:	۵۰۰ نسخه
قیمت	:	۶۰۰۰۰۰۰ ریال

آدرس: تهران، خ شهید مفتح، شماره ۴۳، کدپستی۱۴۹۱۱- ۱۵۷۱۹ تلفن مرکز پخش: ۸۸۳۱۱۸۶۶

www.khu.ac.ir pub@khu.ac.ir

فهرست مطالب

فهرست جداول

مقدمه

ژئوپلیتیک، یکی از شاخه های تخصصی رشته جغرافیای سیاسی است که رابطه متقابل جغرافیا و سیاست را در پرتو قدرت مورد مطالعه قرار می دهد. جغرافیای سیاسی به عنوان زیر مجموعه علم جغرافیا در اواسط قرن ۱۸ میلادی توسط دو فیلسوف معروف فرانسوی و آلمانی بنام های رابرت تورگو و ایمانوئل کانت مفهوم پردازی شد.

ژئوپلیتیک در اواخر قرن ۱۹ میلادی توسط شلین (کیلن) استاد دانشگاه آپسالای سوئد که تحت تاثیر آموزه های فریدریش راتزل جغرافیدان سیاسی آلمانی قرار داشت، وضع و مفهوم پردازی شد. از آن زمان تا کنون جغرافیای سیاسی و ژئوپلیتیک مانند هر نظام علمی دیگر دچار تحول گردیده و ابعاد تخصصی و معرفتی آن گسترش یافته است.

در راستای تحولات دگرگون ساز زندگی بشر و شکل گیری شبکه جهانی اینترنت، فضای جدیدی تحت عنوان فضای مجازی ظهور پیدا کرد و به سرعت بر تمام ابعاد و شئونات زندگی بشر سایه افکند. بطوریکه امروزه حیات بشری بشدت به فضای مجازی وابسته شده و این وابستگی در آینده نیز گسترش بیشتری خواهد یافت که اگر سیاستمداران، معماران و طراحان فضای مجازی مراقبت ننمایند، در آینده ای نه چندان دور بشریت شاهد گرفتار شدن در نوع جدیدی از دیکتاتوری خواهد بود که بنده از آن به **دیکتاتوری دیجیتال** یاد می کنم. فضای مجازی از یک سو امکانات زیادی در اختیار حکومت ها قرار می دهد تا شهروندان را به کنترل و فرمانبری وادارند و اراده خود را به راحتی بر آن ها تحمیل نمایند، و از دیگر سو به شهروندان فرصت هایی می دهد تا حکومت ها را به چالش بکشند و تغییرات اجتماعی، سیاسی و فضایی مورد نظر خود را عملی نمایند.

فضای مجازی از ظرفیتها و فرصتهای تولید قدرت برخوردار است، به عبارتی مانند بقیه فضاهای جغرافیایی ذاتی قدرت آفرین دارد. بر این اساس فضای مجازی برای بازیگران سیاسی و اجتماعی و شکارچیان فرصتهای قدرت، جذاب و وسوسه انگیز است. بنابراین به آوردگاه رقابت، همگرایی، واگرایی، صلح، همکاری، جنگ، ستیز و غیر آن بین بازیگران مختلف اعم از شهروندان، احزاب،

حکام، فرمانروایان، کشورها، نهادهای ملی و بین المللی تبدیل شده است.

از آنجاییکه موضوع جغرافیای سیاسی را مطالعه بعد سیاسی فضای جغرافیایی در مقیاسها و گونه‌های مختلف تشکیل می دهد، با ظهور و گسترش فضای مجازی به عنوان سایه فضای جغرافیایی واقعی، ضرورت مطالعه بعد سیاسی این فضای جدید در قلمرو معرفتی جغرافیای سیاسی مطرح گردیده است. با توجه به اینکه بعد سیاسی فضای مجازی با مولفه قدرت آمیخته و پیوند خورده، بنابراین ژئوپلیتیک فضای مجازی در قلمرو جغرافیای سیاسی ضرورت و موضوعیت پیدا می کند.

با توجه به گسترش خارق العاده فضای مجازی و نقش بنیادی آن در همه شئونات زندگی ابنای بشر، لازمست جغرافیدانان سیاسی بیش از پیش به آن توجه نموده و به کاوش در موضوعات جغرافیای سیاسی و ژئوپلیتیک در فضای مجازی بپردازند، و یافته های خود را برای بهره برداری در معرض دید علاقمندان قرار دهند.

همت و پشتکار استادان ارجمند و همکاران عزیز: جناب آقای دکتر افشین متقی دستنائی و جناب آقای دکتر علی کرمی در تالیف و خلق اثری بدیع و ارزشمند در حوزه جغرافیای سیاسی فضای مجازی تحت عنوان «**عمق ژئوپلیتیک دیجیتال**» گامی بزرگ در این زمینه می باشد، که کمک زیادی به تقویت ادبیات و قلمرو معرفتی جغرافیای سیاسی می نماید. بنده به سهم خودم صمیمانه از آنان تشکر و قدردانی می نمایم.

امیدوارم حاصل کار و تلاش آن ها مورد بهره برداری علاقمندان بویژه اساتید و دانشجویان ارجمند رشته جغرافیای سیاسی در دانشگاه ها قرار بگیرد.

دکتر محمدرضا حافظ‌نیا
تهران- مردادماه ۱۴۰۳

پیشگفتار

عمق ژئوپلیتیک مفهومی محوری برای علم ژئوپلیتیک است؛ داشتن عمق ژئوپلیتیک همیشه با نوعی بازدارندگی دفاعی همراه بوده و از سوی دیگر نداشتن آن مساوی با دغدغه توسعه طلبی و به دست آوردن فضای حیاتی و از سوی دیگر معمای امنیتی است. مفهوم عمق ژئوپلیتیک محور تلاش‌های بازیگران پیرامون فضا بوده و هست؛ هر چه فضا بزرگ‌تر و گسترده‌تر و متنوع تر باشد عمق ژئوپلیتیک برتر. اما با تحولات فناوری‌های اطلاعاتی و ارتباطی نیمه دوم قرن بیستم شاهد دگرگونی مفهوم فضا و به تبع آن مفهوم عمق ژئوپلیتیک هستیم. انقلاب دیجیتال عصر جدیدی را آغاز کرده است که در آن قدرت و ابزار کسب، حفظ و گسترش آن به کلی بازتعریف شده است. همان طور که ابزارهای دیجیتال به طور اجتناب ناپذیری همه جنبه‌های ارتباطات را دگرگون می‌کنند، به طور چشمگیری حوزه‌های سیاسی و اجتماعی- اقتصادی را نیز دوباره پیکربندی می‌کنند. فضای دیجیتال محیط در حال ظهوری است که اینترنت و اتصال داده در آن وجود دارد. این حوزه جدید، فضای سنتی ژئوپلیتیک را به چالش می‌کشد و چالش‌های جدیدی را برای روابط بین الملل ایجاد می‌کند؛ بازیگران سنتی در حال رقابت برای قدرت در این قلمرو ناشناخته به استفاده از استراتژی‌های سنتی ژئوپلیتیک و ژئواکونومیک در دنیای دیجیتال ادامه می‌دهند. این تقلا برای تسلط بر نهادی بدون حاکمیت متمرکز و یا استانداردهای بین‌المللی یا سیاست‌های دسترسی و استفاده، ماهیت اینترنت را بازتعریف می‌کند. دولت‌ها به طور فزاینده‌ای تلاش می‌کنند تا اینترنت و دامنه‌های دیجیتال را برای اهداف استراتژیک ملی تابع خود کنند. استفاده از سلاح‌های سایبری و انجام حملات سایبری، مانند احتمال حمله به زیرساخت‌های حیاتی یا کمپین‌های اطلاعات نادرست چشم‌انداز تهدیدات بین‌المللی را گسترده نموده است. در حالی که این تهدیدات جدید افزایش می‌یابد، دولت‌ها به طور گسترده آمادگی مقابله با این چالش‌های جدید در حوزه دیجیتال را ندارند.

بنابراین بعد دیگری علاوه بر زمینی، هوایی، دریایی و فضایی به فضا اضافه می‌شود به نام فضای دیجیتال و به تبع قدرت دیجیتال ملی. قدرت دیجیتال ملی به توانایی و نفوذ کلی یک کشور در حوزه امنیت سایبری و عملیات سایبری اشاره دارد. قدرت دیجیتال ملی برای حفاظت از امنیت ملی، حفاظت از زیرساخت‌های حیاتی، حفظ ثبات اقتصادی و اطمینان از تاب آوری سیستم‌های دیجیتال در دنیایی که به طور فزاینده‌ای به هم پیوسته و وابسته به ابزارها و ارتباطات دیجیتال است، ضروری

است. این وضعیت نیاز به یک رویکرد کل نگر دارد که ابعاد فناوری، سیاسی، حقوقی و انسانی امنیت سایبری را ادغام کند. مولفه‌های تشکیل دهنده قدرت دیجیتال ملی عبارت‌اند از:۱- زیرساخت: قدرت دفاعی دیجیتال یک کشور، از جمله توانایی آن در شناسایی، پیشگیری و پاسخ به تهدیدات سایبری که دولت، ارتش، زیرساخت‌های حیاتی، مشاغل و افراد را هدف قرار می‌دهد. ۲- هوش دیجیتال: ظرفیت جمع‌آوری، تجزیه و تحلیل و استفاده از اطلاعات مرتبط با تهدیدات دیجیتال، از جمله فعالیت‌های عوامل مخرب، آسیب‌پذیری‌ها در سیستم‌های دیجیتال، و خطرات نوظهور امنیت دیجیتال. ۳- عملیات سایبری: توانایی انجام عملیات سایبری تهاجمی مانند جاسوسی سایبری، خرابکاری و جنگ، و همچنین عملیات سایبری دفاعی برای حفاظت از منافع ملی و پاسخ به تهدیدات سایبری. ۴- سیاست و استراتژی سایبری: توسعه و اجرای سیاست‌ها، استراتژی‌ها و مقررات ملی امنیت برای مقابله با تهدیدات سایبری، حفاظت از زیرساخت‌های حیاتی، ارتقای همکاری بین‌المللی و اطمینان از تاب آوری سیستم‌های دیجیتال.۵- قابلیت‌های دفاع سایبری: استقرار فناوری‌ها، ابزارها و پرسنل امنیت سایبری برای دفاع در برابر حملات سایبری، از جمله سیستم‌های تشخیص نفوذ، فایروال‌ها، مکانیسم‌های رمزنگاری و تیم‌های واکنش به حادثه.۶- تاب آوری دیجیتال: ظرفیت مقاومت در برابر حوادث سایبری، از جمله نقض داده‌ها، حملات باج‌افزار و حملات انکار سرویس با اجرای اقدامات امنیت سایبری قوی و طرح‌های اضطراری. ۷- آموزش دیجیتال و توسعه نیروی کار: سرمایه گذاری در آموزش امنیت دیجیتال و سایبری، آموزش، و توسعه نیروی کار برای پرورش نیروی کار ماهر در امنیت سایبری که قادر به مقابله با تهدیدات سایبری در حال تحول و حفظ قابلیت‌های سایبری ملی باشد. ۸- تعامل بین‌المللی: همکاری با سایر کشورها، سازمان‌های بین‌المللی و نیز شرکای بخش خصوصی برای ارتقای همکاری در زمینه امنیت دیجیتال، اشتراک گذاری اطلاعات تهدیدات، ایجاد هنجارهای امنیت دیجیتال و پاسخ به تهدیدات سایبری فرامرزی.

در دنیای مدرن قدرت دیجیتال ملی یا توانایی یک کشور در حوزه دفاع و تهاجم سایبری، به طور فزاینده‌ای اهمیت یافته است. حملات سایبری به زیرساخت‌های حیاتی تا سیستم‌های نظامی، تهدیدی مهم برای امنیت ملی محسوب می‌شود. داشتن قدرت سایبری قوی برای دفاع در برابر این تهدیدات و بازدارندگی دشمنان ضروری است. حملات سایبری می‌تواند کسب‌وکارها، سیستم‌های

مالی و زنجیره تامین را مختل کند و باعث بی ثباتی اقتصادی شود. کشوری با قابلیت‌های امنیت سایبری قوی می‌تواند از اقتصاد خود در برابر چنین اختلالاتی محافظت کند و قدرت رقابت خود را در بازار جهانی حفظ کند. بسیاری از خدمات ضروری مانند شبکه‌های برق، شبکه‌های حمل و نقل و سیستم‌های مراقبت‌های بهداشتی به سیستم‌های دیجیتال به هم پیوسته متکی هستند. جاسوسی سایبری و سرقت مالکیت معنوی تهدیدهای رایج در عصر دیجیتال هستند. اقدامات امنیتی سایبری قوی برای محافظت از داده‌های حساس، اسرار تجاری و فناوری‌های خاص در برابر به خطر افتادن یا سرقت توسط بازیگران خارجی ضروری است. قابلیت‌های سایبری یک کشور می‌تواند با نشان دادن توانایی آن در مقابله به مثل موثر در فضای سایبری به عنوان یک عامل بازدارنده در برابر دشمنان احتمالی عمل کند. این موضوع می‌تواند به جلوگیری از حملات سایبری و جلوگیری از اقدامات خصمانه‌ای که ممکن است به درگیری‌های متعارف تبدیل شود، کمک کند. همچنین کشورهای دارای قابلیت‌های سایبری پیشرفته می‌توانند از طریق شکل دادن به هنجارهای امنیت سایبری، مشارکت در دیپلماسی سایبری بین‌المللی و همکاری با متحدان برای مقابله با تهدیدات سایبری رایج، بر صحنه جهانی تأثیر بگذارند. در داخل هم اقدامات موثر امنیت سایبری برای حفظ اعتماد عمومی به سیستم‌های دیجیتال و حفاظت از حقوق حریم خصوصی افراد ضروری است. شهروندان از دولت‌هایشان انتظار دارند که از داده‌های شخصی آن‌ها محافظت کرده و تراکنش‌های آنلاین را ایمن کنند. همچنین سرمایه گذاری در تحقیق و توسعه امنیت سایبری، نوآوری و پیشرفت فناوری را در این زمینه تقویت می‌کند. این اقدام نه تنها دفاع سایبری یک کشور را تقویت می‌کند، بلکه به قدرت کلی فن آوری آن نیز کمک می‌کند.

اندازه‌گیری قدرت دیجیتال یک کشور شامل ارزیابی عوامل مختلف مرتبط با قابلیت‌ها، آمادگی و تاب آوری امنیت دیجیتال و سایبری یک کشور است. در حالی که هیچ معیار یا شاخص واحدی وجود ندارد که بتواند قدرت سایبری یک کشور را به طور کامل نشان دهد، مولفه‌هایی مانند زیرساخت امنیت سایبری، قابلیت‌های واکنش به حوادث سایبری، سرمایه گذاری در دفاع سایبری، حفاظت از زیرساخت‌های حیاتی، توانایی کشور برای جمع آوری، تجزیه و تحلیل و به اشتراک گذاری اطلاعات تهدیدات سایبری با شرکای داخلی و بین المللی، آموزش امنیت سایبری و توسعه نیروی کار و همکاری بین المللی در این باره مورد سنجش قرار می‌گیرد.

از طرف دیگر در این فضا عمق ژئوپلیتیک نیز تفسیر تازه‌ای پیدا می‌کند. با رشد و توسعه فضای مجازی شاهد تولد مفهوم جدیدی با نام عمق ژئوپلیتیک دیجیتال هستیم که در آن ابزارهای عمق ژئوپلیتیک کلاسیک دیگر کارگشا نبوده و بعضا حتی مولفه‌های شکل دهنده به آن، عمق و گستردگی عمق ژئوپلیتیکی کلاسیک را ندارند. عمق ژئوپلیتیک دیجیتال مفهومی است هم کمی و کیفی. برای تعمیق عمق ژئوپلیتیک دیجیتال هم بایستی به رشد زیرساخت‌های فنی فضای مجازی توجه کرد و هم توسعه و آموزش نیروی انسانی و تعمیق سواد دیجیتال و سواد رسانه ای. در عمق ژئوپلیتیک دیجیتال وسعت، منابع، تنوع جغرافیایی و نیز جمعیت و ... به تنهایی عامل قدرت نیستند بلکه برعکس شاهدیم که دولت‌های کوچکی که از مولفه‌های فوق الذکر چندان برخوردار نیستند و فاقد عمق ژئوپلیتیک هستند اما از لحاظ مولفه‌های عمق ژئوپلیتیک دیجیتال در رتبه‌های بالا قرار دارند. از جمله مولفه‌های عمق ژئوپلتیک دیجیتال می‌توان به برخورداری از زیرساخت‌های فنی پیشرفته، نیروی انسانی متخصص و آموزش یافته، اینترنت با کیفیت و گسترده و مشارکت بالای شهروندان داری سواد دیجیتال و سواد رسانه‌ای اشاره کرد. با توجه به این مهم در این کتاب قصد داریم مفهوم عمق ژئوپلیتیک دیجیتال را در مقایسه با مفهوم عمق ژئوپلیتیک در معنای کلاسیک تبیین نمائیم.

عمق ژئوپلیتیک دیجیتال شاهراهیست فضایی که نمایانگر قدرت دیجیتال ملی کشورهاست. این ترکیب اصطلاحی محل تقاطع فضاهاست؛ فضای مجازی، فضای سایبری، فضای جغرافیایی، فضای سیاسی و فضای استراتژیک. به طور کلی تصوری روح مانند از فضای دیجیتال وجود داشته و دارد؛ دیده نمی شود و قدرت دخل و تصرف در تحولات فضایی را ندارد یا این که یکی از دعواهای رایج این است که فضای دیجیتال واقعی است اما واقعیت ندارد. اما استفاده تهاجمی و تدافعی از فضای دیجیتال همان اثبات واقعیت داشتن آن است.

ژئوپلیتیک، علمی میان رشته‌ای است که دائما در حال تولید مشترک با رشته‌های دیگر است و از این طریق پسوندها و پیشوندهای گوناگون بدان اضافه می گردد. این ویژگی نشان از خطیر بودن دانش ژئوپلیتیک و نیز پویایی آن در زمان است. عمق ژئوپلیتیک یکی از این ترکیبات است که حاصل آمیختگی ژئوپلیتیک و علوم استراتژیک است. اما این مفهوم برای حفظ پویایی در کنار

تداوم موضوعیت ناچار است برخی الزامات زمانه را نیز در خود جای دهد. فضای دیجیتال یکی از مهم ترین این الزامات است. اینجاست که شاهد بازترکیب عمق ژئوپلیتیک با فضای دیجیتال و شکل گیری ترکیبی جدید با نام عمق ژئوپلیتیک دیجیتال هستیم.

عمق ژئوپلیتیک دیجیتال مفهومی فضایی، سیاسی و نظامی است در حالی که عمق ژئوپلیتیک سنتی بیشتر جغرافیایی(مکانی)، سیاسی و نظامی می نماید. توضیح این که مفاهیم فضا و مکان در مطالعات جغرافیایی متمایز و در عین حال به هم پیوسته هستند. فضا به ابعاد فیزیکی یا مجازی اطلاق می‌شود که در آن رویدادها رخ می‌دهند و اشیا و افراد وجود دارند. مکان اغلب بر حسب فواصل، مختصات و مرزهای فیزیکی توصیف می‌شود. فضا به طور کلی خنثی یا خالی از معنای خاص در نظر گرفته می‌شود تا زمانی که فعالیت‌ها یا ادراکات انسان به آن اهمیت بدهد. فضای بین دو ساختمان یا فضای درون یک اتاق نمونه‌هایی هستند که ابعاد فیزیکی بدون معنای ذاتی تعریف می‌شوند. مکان فضایی است که با فعالیت‌ها و نحوه ادراک افراد در آن معنا یافته است. مکان‌ها آمیخته به اهمیت فرهنگی، اجتماعی و عاطفی هستند که آن‌ها را از یکدیگر متمایز می‌کند. آن‌ها به شکل گیری هویت و حافظه برای افراد و جوامع کمک می‌کنند. فضا انتزاعی‌تر و کلی‌تر است، در حالی که مکان مشخص‌تر و خاص تر. فضا تا زمانی که از طریق تجربه و ادراک انسان به مکانی تبدیل شود فاقد معنای ذاتی است. مکان‌ها محل وقوع فعالیت‌های انسانی و شکل گیری روابط اجتماعی هستند، در حالی که فضا پس‌زمینه‌ای است که این فعالیت‌ها در آن صورت می گیرد. در اصل، فضا بومی را فراهم می‌کند که مکان‌ها از طریق تعامل و تجربه انسانی بر روی آن ایجاد می‌شوند.

سوال اساسی عمق ژئوپلیتیک دیجیتال این است که چرا یک کشور دارای عمق ژئوپلیتیک دیجیتال عمیق تری است و این که مولفه‌های تشکیل دهنده عمق ژئوپلتیک دیجیتال کدام‌اند. در پاسخ به این پرسش پژوهش پیش رو معتقد است که عمق ژئوپلیتیک دیجیتال متشکل از مولفه‌هایی است که سنجش و مقایسه کمی و کیفی آن‌ها تعیین کننده سطح عمق ژئوپلیتیک دیجیتال یک واحد سیاسی است. مهم ترین این مولفه‌ها عبارت‌اند از: کمیت و کیفیت اینترنت به طور قابل توجهی

بر عمق ژئوپلیتیک دیجیتال یک کشور تأثیر می‌گذارد و بر ابعاد اقتصادی، سیاسی، اجتماعی و فناورانه آن تأثیر می‌گذارد. اینترنت با کیفیت بالا به کسب‌وکارها اجازه می‌دهد تا به طور کارآمد فعالیت کنند، نوآوری را تقویت کرده و دسترسی به بازارهای جهانی را ممکن می‌سازد. کشورهای دارای زیرساخت اینترنتی قوی می‌توانند از تجارت الکترونیک، فین تک و سایر صنایع دیجیتال پشتیبانی کنند، سرمایه گذاری خارجی را جذب کنند زیرا شرکت‌ها مناطق با زیرساخت دیجیتال قوی را برای راه اندازی کسب و کار ترجیح می‌دهند. اینترنت سریع و قابل اتکا با برقراری ارتباط کارآمد، کاهش زمان خرابی و تسهیل کار از راه دور، بهره وری را افزایش می‌دهد که می‌تواند منجر به تاب آوری نیروی کار شود. کشورهایی با قابلیت‌های دیجیتال پیشرفته می‌توانند تأثیر بیشتری در صحنه جهانی داشته‌باشند. می‌توانند در سیاست گذاری دیجیتال بین المللی شرکت کنند و از منافع خود دفاع کنند. زیرساخت قوی اینترنت برای امنیت ملی بسیار مهم است. حفاظت بهتر در برابر تهدیدات سایبری را امکان پذیر می‌کند که برای حفظ ثبات سیاسی و حفاظت از اطلاعات حیاتی ضروری است. دسترسی به اینترنت با کیفیت بالا فرصت‌های آموزشی را افزایش می‌دهد و امکان دسترسی به منابع آنلاین، دوره‌ها و ابزارهای مشارکتی را فراهم می‌کند. این موضوع به ایجاد جمعیتی با سواد دیجیتال کمک می‌کند که برای رشد کشور حیاتی است. پزشکی از راه دور و سیستم‌های اطلاعات سلامت بر اتصال قوی به اینترنت تکیه می‌کنند و دسترسی به خدمات مراقبت‌های بهداشتی را به‌ویژه در مناطق دورافتاده بهبود می‌بخشند. اینترنت با کیفیت بالا به پر کردن شکاف دیجیتال کمک و تضمین می‌کند که همه اقشار جامعه بتوانند در اقتصاد دیجیتال مشارکت کنند و به خدمات ضروری دسترسی داشته باشند. همچنین برای فعالیت‌های تحقیق و توسعه بسیار مهم است زیرا به محققان اجازه می‌دهد تا در سطح جهانی با یکدیگر همکاری کنند، به حجم وسیعی از داده‌ها دسترسی داشته باشند و از منابع اینترنتی استفاده کنند. یک زیرساخت اینترنتی قوی از رشد استارت‌آپ‌های فناوری و مراکز نوآوری پشتیبانی می‌کند و به شکل گیری یک اکوسیستم فن‌آوری فعال کمک می‌کند. همچنین توسعه شهرهای هوشمند و برنامه‌های کاربردی اینترنت اشیا به اتصال

به جریان اینترنت پرسرعت و مداوم بستگی دارد زیرا می‌تواند مدیریت شهری را بهبود بخشد و کیفیت زندگی را افزایش دهد. کشورهای دارای اینترنت قوی می‌توانند با تولید و توزیع محتوای دیجیتال در سطح جهانی به نیروگاه‌های فرهنگی تبدیل شوند. محتوای دیجیتال می‌تواند شامل سرگرمی، اخبار و محتوای آموزشی باشد که بر فرهنگ و ارزش‌های جهانی تأثیر می‌گذارد. پلتفرم‌های دیجیتال می‌توانند برای نمایش فرهنگ، ارزش‌ها و ایدئولوژی‌های یک کشور و تقویت قدرت نرم آن در صحنه بین‌المللی استفاده شوند. مثلا کره جنوبی که در جهان با کمیت و کیفیت بالای اینترنت شناخته شده، از این امر برای تبدیل شدن به یک رهبر در فناوری، سرگرمی (به عنوان مثال کی پاپ و بازی) و خدمات دیجیتال استفاده کرده است. یا کشور استونی با ابتکارات دولت الکترونیک و جامعه دیجیتال نشان داده است که چگونه اینترنت با کیفیت بالا می‌تواند خدمات عمومی و مشارکت مدنی را متحول کند. این مثال ها نشان می‌دهند که چگونه سرمایه گذاری‌های قابل توجه در زیرساخت‌های اینترنتی می‌تواند از نوآوری‌های تکنولوژیکی، رشد اقتصادی و نفوذ جهانی حمایت کند. بنابراین کمیت و کیفیت زیرساخت برای عمق ژئوپلیتیک دیجیتال یک کشور اساسی است و بر رونق اقتصادی، ثبات سیاسی، توسعه اجتماعی، نوآوری تکنولوژیک و نفوذ فرهنگی تأثیر می‌گذارند. کشورهایی که روی زیرساخت‌های اینترنتی با کیفیت بالا سرمایه‌گذاری می‌کنند و آن ها را در اولویت قرار می‌دهند در واقع خود را به عنوان پیشرو در عصر دیجیتال می‌شناسانند.

مولفه بعدی امنیت سایبری است. امنیت سایبری نقش مهمی در عمق ژئوپلیتیک دیجیتال یک کشور ایفا می‌کند و بر ثبات اقتصادی، امنیت ملی، جایگاه بین‌المللی و انعطاف‌پذیری اجتماعی آن تأثیر می‌گذارد. اقدامات امنیت سایبری قوی از بانک‌ها و مؤسسات مالی در برابر حملات سایبری محافظت می‌کند و ثبات و یکپارچگی سیستم‌های مالی را تضمین می‌کند. کسب‌وکارها بیشتر در محیط‌هایی فعالیت می‌کنند که احساس کنند دارایی‌های دیجیتالشان امن است. امنیت سایبری قوی باعث افزایش اعتماد و اطمینان سرمایه گذاران داخلی و خارجی می‌شود. زیرا حملات سایبری به دلیل سرقت مالکیت معنوی، اختلال در عملیات و آسیب به اعتبار برندها می‌تواند منجر به خسارت

های اقتصادی قابل توجهی شود. امنیت سایبری قوی این خطرات را به حداقل می‌رساند. کشورها و ملت‌ها با تهدیدات ناشی از جنگ سایبری روبرو هستند، جایی که دشمنان از حملات سایبری برای مختل کردن زیرساخت‌های حیاتی، سرقت اطلاعات حساس یا انجام جاسوسی استفاده می‌کنند. امنیت سایبری موثر برای دفاع در برابر این تهدیدات ضروری است. زیرساخت‌های حیاتی مانند شبکه‌های برق، سیستم‌های تامین آب و شبکه‌های ارتباطی باید در برابر حملات سایبری محافظت شوند. تضمین امنیت این سیستم‌ها برای امنیت ملی و امنیت عمومی حیاتی است. عملیات های نظامی مدرن به شدت به سیستم‌های دیجیتال برای ارتباطات، اطلاعات و تسلیحات متکی هستند. کشورهایی با قابلیت‌های امنیت سایبری پیشرفته می‌توانند سیاست‌ها و استانداردهای سایبری جهانی را تحت تأثیر قرار دهند و خود را به عنوان رهبران حوزه دیجیتال قرار دهند. امنیت سایبری قوی توانایی کشور را برای ایجاد و حفظ اتحادها و مشارکت‌های استراتژیک افزایش می‌دهد. این کشورها به عنوان شرکای قابل اعتماد در همکاری‌های بین المللی و توافق نامه‌های دفاعی دیده می‌شوند. نشان دادن تخصص در امنیت سایبری می‌تواند قدرت نرم یک کشور را تقویت کند. همچنین با ارائه خدمات امنیت سایبری به سایر کشورها، یک کشور می‌تواند حسن نیت دیپلماتیک ایجاد کند و روابط بین المللی دوجانبه را تقویت کند. حفاظت از مالکیت معنوی در برابر سرقت سایبری برای حفظ مزیت رقابتی کشور در فناوری، تحقیق و نوآوری بسیار مهم است. شرکت‌ها و مؤسسات تحقیقاتی در صورتی که معتقد باشند نوآوری هایشان در برابر تهدیدات سایبری محافظت می‌شود، احتمال بیشتری برای سرمایه گذاری در تحقیق و توسعه دارند. تضمین امنیت داده‌های شخصی و محافظت از شهروندان در برابر جرائم سایبری برای حفظ اعتماد عمومی به خدمات و فناوری‌های دیجیتال ضروری است. امنیت سایبری موثر به یک کشور این امکان را می‌دهد که به سرعت و به طور موثر به حوادث سایبری واکنش نشان دهد و تأثیر آن ها را به حداقل برساند و به بهبود سریع شرایط پس از حمله کمک کند. ارتقاء آگاهی و آموزش امنیت سایبری در میان مردم، انعطاف پذیری جامعه را در برابر تهدیدات سایبری افزایش می‌دهد. از آنجایی که کشورها دستخوش تحول دیجیتال می‌شوند، امنیت سایبری تضمین می‌کند که فناوری‌ها و سیستم‌های جدید به طور ایمن و بدون ایجاد آسیب پذیری‌های جدید به کار گرفته شوند. یک محیط دیجیتال امن، نوآوری را با فراهم کردن فضای امن برای استارتاپ‌ها و شرکت‌های فناوری برای توسعه محصولات و خدمات

جدید تقویت می‌کند. به عنوان مثال رژیم صهیونیستی اسرائیل (فلسطین اشغالی) که به صنعت پیشرفته امنیت سایبری خود معروف است از این تخصص خود برای تبدیل شدن به یک رهبر جهانی در فناوری و سیاست امنیت سایبری استفاده کرده است. یا مثلا ایالات متحده دارای قابلیت‌های قابل توجهی در امنیت سایبری است، با ابتکاراتی مانند آژانس امنیت سایبری و امنیت زیرساخت برای محافظت از زیرساخت‌های حیاتی و پاسخ به تهدیدات سایبری. استونی پس از حمله سایبری بزرگ در سال ۲۰۰۷ میلادی، به الگویی برای ایجاد یک جامعه دیجیتالی تاب آور با اقدامات امنیتی سایبری قوی تبدیل شده است. امنیت سایبری جزء لاینفک عمق ژئوپلیتیک دیجیتال یک کشور است. زیرا پایه ثبات اقتصادی، امنیت ملی و انعطاف پذیری اجتماعی است و در عین حال جایگاه و نفوذ بین المللی یک کشور را تقویت می‌کند. کشورهایی که امنیت سایبری را در اولویت قرار می‌دهند، برای محافظت از دارایی‌های دیجیتالی خود، تقویت نوآوری و حفظ مزیت رقابتی خود در چشم انداز دیجیتال جهانی، موقعیت بهتری دارند.

زیرساخت‌های سایبری تاب آور سنگ بنای قدرت دیجیتال یک کشور است که آن را قادر می‌سازد تا در برابر تهدیدات و اختلالات سایبری مقاومت کند، پاسخ دهد و توان خود را بازیابی کند. زیرساخت سایبری تاب آور تضمین می‌کند که کسب‌وکارها می‌توانند حتی در مواجهه با حملات سایبری به فعالیت خود ادامه دهند. این تداوم برای حفظ ثبات و رشد اقتصادی بسیار مهم است. همان طوری که گفته شد سرمایه‌گذاران بیشتر در کشورهایی با زیرساخت‌های سایبری قوی و تاب آور سرمایه‌گذاری می‌کنند، زیرا خطر اختلالات اقتصادی ناشی از حوادث سایبری را کاهش می‌دهد. محیط‌های سایبری تاب آور با ایجاد فضایی امن برای توسعه و استقرار فناوری‌ها و خدمات جدید، نوآوری را تقویت می‌کند. از خدمات ضروری مانند انرژی، آب، حمل و نقل و مراقبت‌های بهداشتی در برابر تهدیدات سایبری محافظت می‌کند و تضمین می‌کند که این خدمات در طول بحران‌ها عملیاتی باقی می‌مانند. سیستم‌های نظامی و دفاعی برای عملکرد مؤثر به زیرساخت‌های سایبری ایمن و انعطاف‌پذیر متکی هستند. این تاب آوری برای عملیات‌های دفاعی و امنیتی ملی حیاتی است. یک زیرساخت دیجیتال تاب آور می‌تواند حملات سایبری را شناسایی، مدیریت و توان خود را مجددا بازیابی کند و کشور را در برابر تاکتیک‌های جنگ سایبری مورد استفاده دشمنان محافظت کند.

تضمین امنیت و حریم خصوصی داده‌های شهروندان برای حفظ اعتماد اجتماعی و جلوگیری از نقض داده‌ها و جرایم سایبری بسیار مهم است. زیرساخت‌های انعطاف‌پذیر پاسخ و بازیابی مؤثر حوادث سایبری را ممکن می‌سازد، اختلالات اجتماعی را به حداقل می‌رساند و در دسترس قرار گرفتن مجدد خدمات را تضمین می‌کند. زیرساخت تاب‌آور از توسعه و استقرار ایمن فناوری‌های نوظهور مانند هوش مصنوعی، اینترنت اشیا و بلاک چین پشتیبانی می‌کند. یک محیط دیجیتال امن و انعطاف‌پذیر، یک اکوسیستم نوآوری پررونق را تقویت می‌کند و از استارت‌آپ‌ها و شرکت‌های فناوری برای توسعه محصولات و خدمات جدید حمایت می‌کند. زیرساخت سایبری تاب آور از تجارت جهانی ایمن و کارآمد با محافظت از زنجیره تامین و کاهش خطر اختلالات پشتیبانی می‌کند. سرمایه گذاری در زیرساخت‌های انعطاف پذیر باعث رشد صنعت امنیت سایبری، ایجاد شغل و افزایش رقابت اقتصادی می‌شود. یک زیرساخت سایبری قوی از ارائه خدمات دیجیتال قابل اعتماد پشتیبانی می‌کند و مزیت رقابتی کشور را در بازار جهانی افزایش می‌دهد. سنگاپور که به دلیل استراتژی جامع امنیت سایبری شناخته شده است، زیرساخت سایبری انعطاف پذیری را توسعه داده است که از موقعیت آن به عنوان یک مرکز مالی و فناوری جهانی پشتیبانی می‌کند. جامعه دیجیتال استونی برای محافظت از خدمات دولت الکترونیک خود به زیرساخت‌های سایبری انعطاف پذیر متکی است که امنیت ملی و اعتماد عمومی را افزایش می‌دهد. با ابتکاراتی مانند چارچوب امنیت سایبری موسسه ملی استاندارد و فناوری، ایالات متحده بر ایجاد زیرساخت‌های انعطاف پذیر برای حمایت از امنیت ملی و رشد اقتصادی متمرکز است.

استقلال سایبری به معنای توانایی یک کشور برای حفظ و کنترل زیرساخت‌های فضای سایبری، داده‌ها و قابلیت‌های دیجیتال، یکی از جنبه‌های حیاتی عمق ژئوپلیتیک دیجیتال است. این مولفه ابعاد مختلفی از جمله حاکمیت تکنولوژیکی، حاکمیت داده‌ها و ظرفیت دفاع در برابر تهدیدات سایبری و پاسخ به آن را در بر می‌گیرد. استقلال سایبری تضمین می‌کند که یک کشور می‌تواند به طور مستقل سیستم‌های دفاعی خود را بدون اتکا به فناوری خارجی توسعه، مدیریت و محافظت کند. یک کشور با کنترل زیرساخت‌های فضای سایبری خود، بهتر می‌تواند از اطلاعات و ارتباطات حساس در برابر فعالیت‌های جاسوسی محافظت کند. استقلال سایبری توانایی کشور را برای دفاع در برابر جنگ سایبری افزایش می‌دهد و کنترل بیشتری بر عملیات سایبری تهاجمی و تدافعی فراهم

می‌کند. استقلال سایبری به یک کشور این امکان را می‌دهد تا اقتصاد دیجیتال خود را تنظیم و حمایت کند و اطمینان حاصل کند که فعالیت‌های اقتصادی و تراکنش‌های دیجیتال ایمن و در محدوده حاکمیت آن هستند. کنترل مستقل بر فضای سایبری، نوآوری و تحقیق و توسعه داخلی را تشویق می‌کند و بخش فناوری رقابتی و خودپایدار را تقویت می‌کند. استقلال سایبری به محافظت از مالکیت معنوی در برابر سرقت و حملات سایبری خارجی کمک می‌کند و تضمین می‌کند که نوآوری‌ها و فناوری‌های اختصاصی ایمن باقی می‌مانند. توسعه فناوری‌های داخلی، کاهش وابستگی به فناوری خارجی و افزایش قابلیت‌های ملی را به پیش می‌برد. کشورهای دارای استقلال سایبری می‌توانند استانداردها و پروتکل‌های امنیت سایبری خود را ایجاد کنند و اطمینان حاصل کنند که این پروتکل‌ها با منافع ملی و الزامات امنیتی مطابقت دارند. با توسعه و کنترل زیرساخت سایبری خود، یک کشور می‌تواند خطرات مرتبط با اختلالات زنجیره تامین جهانی و وابستگی به خارج را کاهش دهد. استقلال سایبری یک کشور را قادر می‌سازد تا نحوه جمع‌آوری، ذخیره، پردازش و اشتراک‌گذاری داده‌ها را کنترل کند و اطمینان حاصل کند که حاکمیت داده‌ها با قوانین ملی و استانداردهای حفظ حریم خصوصی همسو است. زیرساخت مستقل فضای سایبری حفاظت از داده‌های شخصی شهروندان را در برابر دسترسی غیرمجاز و سوء استفاده افزایش می‌دهد و اعتماد عمومی به خدمات دیجیتال را تقویت می‌کند. کشورها می‌توانند مقررات حفاظت از داده‌های خود را اجرا کنند و اطمینان حاصل کنند که شیوه‌های مدیریت داده در مرزهای آن ها با استانداردهای ملی مطابقت دارد. استقلال سایبری کشور را به عنوان کشوری پیشرو در سیاست و حکمرانی امنیت سایبری جهانی قرار می‌دهد و به آن اجازه می‌دهد بر هنجارها و استانداردهای بین المللی تأثیر بگذارد. با حفظ کنترل بر فضای سایبری خود، یک کشور می‌تواند اهداف استراتژیک خود را بدون تأثیر نابجای قدرت‌های خارجی دنبال کند و استقلال ژئوپلیتیکی خود را افزایش دهد. استقلال سایبری موقعیت یک کشور را در دیپلماسی سایبری تقویت می‌کند و آن را قادر می‌سازد تا اتحادها و مشارکت‌هایی را بر اساس احترام متقابل و منافع مشترک تشکیل دهد. استقلال سایبری اعتماد عمومی را به امنیت و قابلیت اطمینان خدمات و زیرساخت‌های دیجیتال ملی افزایش می‌دهد و مشارکت بیشتر در اقتصاد دیجیتال را تشویق می‌کند. ارتقای استقلال سایبری مستلزم افزایش آگاهی از سواد دیجیتال و امنیت سایبری در میان شهروندان، ایجاد جامعه‌ای انعطاف پذیرتر و آگاه

تر است. کشور دارای استقلال سایبری مجهزتر برای مدیریت و بازیابی حوادث سایبری، تضمین تداوم خدمات ضروری و به حداقل رساندن اختلالات اجتماعی است. به عنوان مثال چین با تمرکز بر استقلال سایبری ابتکاراتی مانند دیوار آتش بزرگ و توسعه فناوری بومی را که هدف آن کنترل فضای سایبری و کاهش وابستگی به فناوری خارجی است را در پیش گرفته است. روسیه بر استقلال سایبری از طریق تلاش برای ایجاد یک اینترنت مستقل تاکید کرده است که امکان کنترل بیشتر بر زیرساخت‌ها و داده‌های دیجیتال را فراهم می‌کند. فشار هند برای حاکمیت دیجیتال شامل ابتکاراتی مانند سیاست محلی سازی داده‌ها و توسعه راه حل‌های فناوری بومی برای افزایش امنیت ملی و انعطاف پذیری اقتصادی است.

نوآوری سایبری یعنی توسعه و بکارگیری فناوری‌ها و روش‌های جدید در فضای سایبری که به جنبه‌های مختلف قدرت و نفوذ یک ملت کمک می‌کند نقش مهمی در افزایش عمق ژئوپلیتیک دیجیتال یک کشور ایفا می‌کند. نوآوری سایبری کشور را به عنوان یک پیشرو در فناوری معرفی می‌کند و رشد اقتصادی را از طریق توسعه محصولات و خدمات به روز پیش می‌برد. کشورهایی که در خط مقدم نوآوری سایبری هستند، سرمایه‌گذاری داخلی و خارجی را جذب می‌کنند، اقتصاد خود را تقویت می‌کنند و شغل ایجاد می‌کنند. فناوری‌های نوآورانه سایبری فرآیندهای کسب‌وکار را ساده می‌کند، بهره وری را افزایش می‌دهد و کارایی عملیاتی را در صنایع مختلف بهبود می‌بخشد و با توسعه ابزارهای پیشرفته امنیت سایبری، استراتژی‌های دفاع سایبری و قابلیت‌های تهاجم سایبری، قابلیت‌های دفاعی کشور را افزایش می‌دهد. همچنین شناسایی، پیشگیری و کاهش تهدیدات سایبری، حفاظت از زیرساخت‌های ملی و اطلاعات حساس را امکان‌پذیر می‌سازد. کشور را به ابزارها و استراتژی‌های لازم برای درگیر شدن در جنگ سایبری و دفاع در برابر آن مجهز می‌کند و امنیت ملی را تضمین می‌کند. نوآوری سایبری وابستگی به فناوری‌های خارجی را کاهش می‌دهد و کشور را قادر می‌سازد تا زیرساخت‌ها و قابلیت‌های سایبری خود را توسعه و کنترل کند. با پرورش فرهنگ نوآوری، کشورها می‌توانند مالکیت معنوی را تولید و از آن محافظت کنند و مزیت رقابتی را در بازار جهانی حفظ کنند. نوآوری در فضای دیجیتال به کشورها امکان می‌دهد راه حل‌های سفارشی سازی شده‌ای را توسعه دهند که نیازهای خاص و الزامات امنیتی آنها را برآورده کند. کشورهایی که در نوآوری سایبری پیشرو هستند، می‌توانند بر استانداردها، سیاست‌ها و بهترین

شیوه‌های جهانی تأثیر بگذارند و جایگاه بین‌المللی خود را افزایش دهند. با به اشتراک گذاشتن نوآوری‌ها و تخصص‌های امنیت سایبری، کشورها می‌توانند اتحاد ایجاد کنند و روابط دیپلماتیک را تقویت کنند و ثبات و همکاری جهانی را ارتقا دهند. همچنین نوآوری سایبری به قدرت نرم یک کشور با نشان دادن مهارت‌های تکنولوژیکی آن و افزایش شهرت آن در صحنه جهانی کمک می‌کند. راه‌حل‌های نوآورانه امنیت سایبری، زیرساخت‌های ملی را در برابر تهدیدات سایبری مقاوم‌تر می‌کنند و خطر اختلالات اقتصادی را کاهش می‌دهند. نوآوری سایبری کشورها را قادر می‌سازد تا به سرعت خود را با پیشرفت‌های فناوری سازگار کنند و تضمین کند که رقابتی و در فضای اقتصاد دیجیتال باقی می‌مانند. یک اکوسیستم نوآوری سایبری قوی، از رشد استارت‌آپ‌ها و شرکت‌های کوچک و متوسط حمایت می‌کند و تنوع اقتصادی و انعطاف‌پذیری را افزایش می‌دهد. نوآوری سایبری ارائه خدمات عمومی مانند مراقبت‌های بهداشتی، آموزش و مدیریت دولتی را بهبود می‌بخشد و کیفیت زندگی را افزایش می‌دهد. کشورهای صاحب نوآوری سایبری می‌توانند شکاف دیجیتال را پر کنند و دسترسی گسترده‌تر به منابع و خدمات دیجیتال را برای همه شهروندان تضمین کنند. ترویج نوآوری سایبری شامل سرمایه‌گذاری در آموزش و خلق نیروی کار ماهر است که قادر به پشتیبانی و ارتقای قابلیت‌های سایبری ملی است. نوآوری سایبری تضمین می‌کند که کشورها کنترل بر زیرساخت‌های حیاتی خود را حفظ می‌کنند، آسیب‌پذیری‌ها را کاهش می‌دهند و استقلال استراتژیک را افزایش می‌دهند. به کشورها این امکان را می‌دهد تا سیاست‌های سایبری مستقلی را توسعه دهند که با منافع ملی و نیازهای امنیتی آنها هماهنگ باشد. نهایتا نوآوری سایبری حاکمیت کشور را در فضای سایبری تقویت می‌کند و آن را قادر می‌سازد از مرزهای دیجیتال خود محافظت کند و حضور خود را در قلمرو دیجیتالی تثبیت کند.

مشارکت مردم با تقویت فرهنگ آگاهی از امنیت سایبری، ارتقاء سواد دیجیتال و تقویت همکاری بین دولت، بخش خصوصی و جامعه مدنی، نقش مهمی در افزایش قدرت سایبری ملی یک کشور ایفا می‌کند. زمانی که مردم از خطرات امنیت سایبری آگاه باشند، بهتر می‌توانند از خود و سازمان هایشان در برابر تهدیدات سایبری محافظت کنند. این آگاهی جمعی آسیب پذیری‌ها را کاهش می‌دهد و تاب آوری سایبری کلی کشور را تقویت می‌کند. مشارکت مردم در برنامه‌های سواد دیجیتال کمک می‌کند تا اطمینان حاصل شود که همه مهارت‌ها و دانش لازم برای استفاده

ایمن و مؤثر از فناوری‌های دیجیتال را دارند. این امر بهداشت کلی سایبری جمعیت را بهبود می‌بخشد و احتمال قربانی شدن در حملات سایبری را کاهش می‌دهد. مشارکت فعال مردم در گزارش رویدادهای سایبری، مانند تلاش‌های فیشینگ یا آلودگی‌های بدافزار، به مقامات کمک می‌کند تا تهدیدات سایبری را به طور مؤثرتری شناسایی کرده و به آنها پاسخ دهند. این تشخیص زودهنگام می‌تواند از حملات سایبری در مقیاس بزرگتر جلوگیری کرده و تأثیر آنها را به حداقل برساند. مردم می‌توانند با داوطلب شدن در سازمان‌های امنیت سایبری، شرکت در تمرین‌های دفاع سایبری یا به اشتراک گذاشتن اطلاعات تهدیدات، به تلاش‌های دفاع سایبری کشور کمک کنند. این تلاش جمعی توانایی کشور را برای دفاع در برابر حملات سایبری افزایش می‌دهد. حمایت و مشارکت مردم از استراتژی‌ها و ابتکارات ملی امنیت سایبری برای موفقیت آنها ضروری است که شامل پیروی از دستورالعمل‌های امنیت سایبری، شرکت در کمپین‌های آگاهی‌بخشی و حمایت از اقدامات امنیت سایبری است. مشارکت مردم در ترویج استفاده مسئولانه از فناوری، مانند رعایت حقوق حریم خصوصی و پرهیز از انتشار اطلاعات نادرست آنلاین، به حفظ محیط دیجیتالی امن‌تر و امن‌تر برای همه کمک می‌کند. مشارکت مردم در نوآوری دیجیتال، مانند توسعه فناوری‌های جدید امنیت سایبری یا ترویج شیوه‌های کدگذاری ایمن، می‌تواند باعث پیشرفت در امنیت سایبری و تقویت قابلیت‌های سایبری کشور شود. در نهایت، مشارکت مردم در تلاش‌های امنیت سایبری به ایجاد فرهنگ امنیت سایبری قوی در داخل کشور کمک می‌کند. این فرهنگ بر اهمیت امنیت سایبری در تمام جنبه‌های جامعه تاکید می‌کند و مسئولیت جمعی برای دفاع سایبری را پرورش می‌دهد. نهاتا می توان گفت که مشارکت مردم برای افزایش عمق ژئوپلیتیک دیجیتال یک کشور ضروری است. با ترویج آگاهی از امنیت سایبری، افزایش سواد دیجیتال، مشارکت در تلاش‌های دفاع سایبری و حمایت از استراتژی‌های امنیت سایبری ملی، مردم می‌توانند به ایجاد یک محیط دیجیتال امن‌تر برای همه کمک کنند.

سواد دیجیتال، توانایی جست و جو، ارزیابی و ایجاد اطلاعات به‌طور مؤثر و انتقادی با استفاده از طیف وسیعی از فناوری‌های دیجیتال، نقش مهمی در افزایش عمق ژئوپلیتیک دیجیتال یک کشور ایفا می‌کند. این نوع سواد شامل طیف گسترده‌ای از مهارت‌ها، از استفاده اولیه از رایانه تا تخصص فنی پیشرفته است و بر ابعاد مختلف قدرت و نفوذ عمق ژئوپلیتیک دیجیتال تأثیر می گذارد. نیروی

کار با سواد دیجیتال برای رشد اقتصادی و رقابت ضروری است. کارگران با مهارت‌های دیجیتال می‌توانند با فناوری‌های جدید سازگار شوند و بهره وری و نوآوری را بهبود بخشند. سواد دیجیتالی فرهنگ نوآوری و کارآفرینی را تقویت می‌کند. افراد با مهارت‌های دیجیتالی می‌توانند استارت آپ ایجاد کنند، فناوری‌های جدید را توسعه دهند و تنوع اقتصادی را پیش ببرند. تقاضا برای مهارت‌های دیجیتال فرصت‌های شغلی جدیدی را در بخش‌هایی مانند فناوری اطلاعات، امنیت سایبری و بازاریابی دیجیتال ایجاد می‌کند و به اشتغال و ثبات اقتصادی کمک می‌کند. سواد دیجیتالی دسترسی به مجموعه وسیعی از منابع آموزشی آنلاین و پلت‌فرم‌های یادگیری را امکان‌پذیر می‌سازد و آموزش مستمر و توسعه مهارت را ارتقا می‌دهد. مهارت در ابزارها و فناوری‌های دیجیتال برای پیشرفت آموزش در علوم، فناوری، مهندسی و ریاضیات که حوزه‌های کلیدی برای توسعه ملی هستند، بسیار مهم است. سواد دیجیتال با فراهم کردن دسترسی همه شهروندان، از جمله کسانی که در مناطق دورافتاده یا محروم هستند، به آموزش و مواد آموزشی باکیفیت، به پر کردن شکاف‌های آموزشی کمک می‌کند. سواد دیجیتالی همچنین شامل درک اصول امنیت سایبری، کمک به افراد و سازمان‌ها برای محافظت از خود در برابر تهدیدات سایبری و کاهش آسیب پذیری کلی زیرساخت‌های ملی است. جمعیتی با سواد دیجیتالی از توسعه و اجرای فن‌آوری‌های دفاعی پیشرفته و استراتژی‌های دفاع سایبری پشتیبانی می‌کنند و امنیت ملی را تقویت می‌دهند. در مواقع بحران، مانند بلایای طبیعی یا حملات سایبری، سواد دیجیتالی ارتباط موثر، اشتراک گذاری اطلاعات و هماهنگی تلاش‌های واکنش را ممکن می‌سازد. سواد دیجیتال شهروندان را برای دسترسی، ارزیابی و به اشتراک گذاری اطلاعات، تقویت مشارکت آگاهانه در فرآیندهای دموکراتیک و افزایش ثبات سیاسی توانمند می‌سازد. استفاده ماهرانه از ابزارهای دیجیتال به شهروندان اجازه می‌دهد تا با خدمات دولت الکترونیک درگیر شوند و کارایی و شفافیت عملیات و خدمات دولت را بهبود بخشند. سواد دیجیتالی شهروندان را برای سازماندهی، حمایت و مشارکت در اهداف اجتماعی و سیاسی، تقویت جامعه مدنی و ترویج عدالت اجتماعی توانا می‌سازد. ترویج سواد دیجیتال تضمین می‌کند که همه شهروندان، از جمله گروه‌های به حاشیه رانده شده و محروم، می‌توانند به طور کامل در جامعه دیجیتال مشارکت کنند و نابرابری‌های اجتماعی را کاهش دهند. ایجاد جوامع آنلاین و شبکه‌های اجتماعی را تسهیل می‌کند، انسجام اجتماعی و اقدام جمعی را تقویت می‌کند. مهارت‌های

دیجیتالی افراد را قادر می‌سازد تا به خدمات ضروری مانند مراقبت‌های بهداشتی، بانکی و خدمات اجتماعی به صورت آنلاین دسترسی داشته باشند و کیفیت زندگی و رفاه اجتماعی را بهبود بخشد. جمعیت با سواد دیجیتالی، رقابت پذیری کشور را در بازار جهانی افزایش می‌دهد و سرمایه گذاری و مشارکت را جذب می‌کند. به کشورها اجازه می‌دهد تا فرهنگ و ارزش‌های خود را در سطح جهانی از طریق پلتفرم‌های دیجیتال به اشتراک بگذارند و قدرت نرم و نفوذ بین المللی خود را افزایش دهند. مهارت در ابزارهای دیجیتال، همکاری بین المللی را در تحقیق، نوآوری و سیاست گذاری تسهیل می‌کند و نقش یک کشور را در امور جهانی تقویت می‌کند. همچنین برای پذیرش فناوری‌های نوظهور مانند هوش مصنوعی، بلاک چین و اینترنت اشیا، که باعث پیشرفت فناوری می‌شود، بسیار مهم است. جمعیت با سواد دیجیتالی از فعالیت‌های تحقیق و توسعه قوی پشتیبانی می‌کند که منجر به پیشرفت‌ها و پیشرفت‌های فناوری می‌شود. مهارت‌های دیجیتالی، تحول صنایع سنتی را از طریق اتخاذ ابزارها و فرآیندهای دیجیتال، افزایش کارایی و رقابت‌پذیری امکان‌پذیر می‌سازد. به عنوان مثال استونی به خاطر خدمات دولت الکترونیکی شناخته می‌شود، سرمایه‌گذاری هنگفتی در سواد دیجیتالی انجام داده است که امکان دسترسی گسترده به خدمات دیجیتال را فراهم کرده و جامعه بسیار مرتبط و آنلاین را تقویت می‌کند. با تمرکز بر فناوری و آموزش، کره جنوبی به سطوح بالایی از سواد دیجیتالی دست یافته است که باعث رشد اقتصادی و رهبری فناوری این کشور شده است. رویکرد جامع فنلاند به سواد دیجیتال، از جمله ادغام آن در سیستم آموزشی، منجر به جمعیتی بسیار ماهر و نوآور برای این کشور شده است.

سواد رسانه‌ای به معنای توانایی دسترسی، تحلیل، ارزیابی و ایجاد رسانه در اشکال مختلف، نقش بسزایی در ارتقای عمق ژئوپلیتیک دیجیتال یک کشور دارد. شهروندان را به مهارت‌های تفکر انتقادی مجهز می‌کند که برای حرکت در چشم‌انداز پیچیده رسانه‌ای، ارتقای تصمیم گیری آگاهانه و تقویت فرآیندهای دموکراتیک ضروری است. شهروندان با سواد رسانه‌ای می‌توانند اخبار و اطلاعات را به طور انتقادی ارزیابی کنند، تصمیمات آگاهانه در طول انتخابات بگیرند و مشارکت مدنی که حکومت دموکراتیک را تقویت می‌کند بروز دهند. سواد رسانه‌ای به افراد کمک می‌کند تا اطلاعات نادرست و تبلیغات را شناسایی کرده و با آن مقابله کنند، از یکپارچگی گفتمان عمومی محافظت می‌کند و آگاهی رای دهندگان را تضمین می‌کند. شهروندانی که به مهارت‌های سواد

رسانه‌ای مجهز هستند، می‌توانند با تحلیل انتقادی گزارش‌های رسانه‌ها و شرکت در بحث‌های عمومی، مقامات و نهادهای دولتی را پاسخگو بدانند.

سواد رسانه‌ای امنیت ملی را با توانمندسازی شهروندان برای شناسایی و مقاومت در برابر عملیات نفوذ خارجی، کمپین‌های اطلاعات نادرست و عملیات روانی افزایش می‌دهد. در مواقع بحران، مانند بلایای طبیعی یا تهدیدات امنیتی، شهروندان با سواد رسانه‌ای می‌توانند به طور موثر به اطلاعات قابل اعتماد دسترسی پیدا کرده و آن‌ها را تفسیر کنند و از پاسخ‌های هماهنگ و آگاهانه حمایت کنند. سواد رسانه‌ای شامل درک خطرات و تهدیدات دیجیتال، ترویج رفتار آنلاین امن تر و کاهش آسیب پذیری در برابر حملات سایبری نیز هست. سواد رسانه‌ای با کمک به شهروندان در ارزیابی انتقادی دیدگاه‌ها و بازنمایی‌های رسانه‌ای، تقویت انسجام اجتماعی و کاهش قطبی‌سازی، درک و مدارا را ارتقا می‌دهد. با ارائه مهارت‌هایی برای هدایت و تولید رسانه، جوامع حاشیه‌نشین را قادر می‌سازد تا نگرانی‌های خود را بیان کنند و به طور کامل در گفتمان اجتماعی مشارکت کنند. به افراد کمک می‌کند سخنان نفرت‌انگیز و کلیشه‌های مضر را بشناسند و به چالش بکشند و به شکل گیری جامعه‌ای فراگیرتر و محترمانه‌تر کمک کنند. مهارت‌های سواد رسانه‌ای در نیروی کار مدرن که توانایی ارزیابی انتقادی و ایجاد رسانه در بسیاری از صنایع ضروری است، به طور فزاینده‌ای ارزشمند است. سواد رسانه‌ای با تشویق افراد به تولید محتوای اصیل و کمک به صنایع فرهنگی و خلاق، خلاقیت و نوآوری را تقویت می‌کند. مصرف کنندگان با سواد رسانه‌ای می‌توانند انتخاب‌های آگاهانه‌تری داشته باشند، تبلیغات گمراه کننده را تشخیص دهند و از خود در برابر تقلب و استثمار محافظت کنند. ادغام سواد رسانه‌ای در آموزش به دانش آموزان کمک می‌کند تا تفکر انتقادی و مهارت‌های تحلیلی را توسعه دهند و عملکرد کلی تحصیلی و آمادگی آنها را برای یادگیری مادام العمر بهبود بخشند. سواد رسانه‌ای مکمل سواد دیجیتال است و مجموعه‌ای از مهارت‌های جامع را برای پیمایش موثر و مسئولانه در دنیای دیجیتال ارائه می‌دهد. سواد رسانه‌ای با آموزش نحوه تعامل انتقادی با رسانه‌ها، درک مسائل مدنی و مشارکت در فرآیندهای دموکراتیک، شهروندی فعال را ترویج می‌کند. کشورهایی که سطح سواد رسانه‌ای بالایی دارند می‌توانند محتوای رسانه‌ای با کیفیتی تولید کنند که بر روایت‌های جهانی تأثیر بگذارد و ارزش‌های فرهنگی و سیاسی آنها را ارتقا دهد. سواد رسانه‌ای از ایجاد و انتشار محتوای فرهنگی حمایت می‌کند و قدرت نرم کشور و نفوذ فرهنگی بین المللی را تقویت می‌کند.

شهروندان و متخصصان با سواد رسانه‌ای می‌توانند در همکاری‌های رسانه‌ای بین المللی شرکت کنند و به تبادل دانش و نوآوری جهانی کمک کنند. سواد رسانه‌ای به سواد سلامت کمک می‌کند که افراد را قادر می‌سازد اطلاعات بهداشتی را به طور انتقادی ارزیابی کنند، تصمیمات بهداشتی آگاهانه بگیرند و اطلاعات نادرست در مورد مسائل بهداشتی را تشخیص دهند. به افراد کمک می‌کند تا در فضای رسانه‌ای به گونه‌ای حرکت کنند که بهزیستی روانی را ارتقا دهد و تأثیر منفی مصرف رسانه‌ها مانند اضطراب و استرس را کاهش دهد. سواد رسانه‌ای با اطمینان از اینکه پیام‌ها به طور انتقادی دریافت می‌شوند، اثربخشی کمپین‌های بهداشت عمومی را افزایش می‌دهد. رویکرد جامع فنلاند برای آموزش سواد رسانه‌ای، آن را به یک رهبر جهانی در مبارزه با اطلاعات نادرست و ترویج شهروندی آگاه تبدیل کرده است. طرح‌های سواد رسانه‌ای کانادا، از جمله ادغام در برنامه‌های درسی مدارس و کمپین‌های آگاهی عمومی، جمعیتی باهوش رسانه را پرورش داده است که قادر به تعامل انتقادی با رسانه‌ها هستند. تاکید استرالیا بر سواد رسانه‌ای از طریق برنامه‌های آموزشی و منابع عمومی، انعطاف‌پذیری اجتماعی آن را در برابر اطلاعات نادرست و افزایش مشارکت دموکراتیک تقویت کرده است.

تولید محتوای دیجیتال با افزایش ابعاد مختلف [illegible]، امنیت، اقتصاد و حضور فرهنگی به عمق ژئوپلیتیک دیجیتال یک کشور کمک قابل توجهی می‌کند. صنعت محتوای دیجیتال که رسانه‌ها، سرگرمی‌ها، بازی‌ها و موارد دیگر را در بر می‌گیرد، محرک قابل توجهی برای رشد اقتصادی و ایجاد شغل است. محتوای دیجیتالی با کیفیت بالا را می‌توان در سطح جهانی توزیع کرد و از بازارهای بین المللی درآمد ایجاد کرد و رقابت اقتصادی را افزایش داد. تولید محتوای دیجیتال، نوآوری در فناوری و توسعه نرم افزار را تقویت می‌کند و به اکوسیستم فناوری گسترده تر کمک می‌کند. محتوای دیجیتال مانند فیلم، موسیقی و بازی‌های ویدئویی می‌تواند به عنوان صادرات فرهنگی، ترویج فرهنگ و ارزش‌های یک کشور در سطح جهانی عمل کند. محتوای دیجیتالی جذاب و تاثیرگذار با شکل دادن به ادراکات جهانی و ایجاد ارتباطات فرهنگی، قدرت نرم یک کشور را افزایش می‌دهد. به حفظ و ارتقای هویت، میراث و ارزش‌های ملی کمک می‌کند و حس وحدت و غرور را در میان شهروندان تقویت می‌کند. تولید محتوای دیجیتالی که به آموزش و افزایش آگاهی در مورد تهدیدات امنیت سایبری و بهترین شیوه‌ها می‌پردازد، عمق ژئوپلیتیک

دیجیتال را افزایش می‌دهد. همچنین محتوای دیجیتال ابزاری در جنگ اطلاعاتی است که در آن محتوای استراتژیک می‌تواند با اطلاعات نادرست مقابله کند، بر افکار عمومی تأثیر بگذارد و روایت‌های ملی را اثبات کند. پلت‌فرم‌های محتوای دیجیتال با کیفیت بالا و ایمن، اتکا به رسانه‌ها و فناوری خارجی را کاهش می‌دهند و امنیت و انعطاف‌پذیری ملی را افزایش می‌دهند.

محتوای دیجیتال که اخبار دقیق، مطالب آموزشی و اطلاعات مدنی را ارائه می‌کند، شهروندان را قادر می‌سازد تا تصمیم‌گیری آگاهانه و مشارکت در حکمرانی داشته باشند. پلت‌فرم‌های محتوای دیجیتال گفتگو و تعامل بین شهروندان و دولت را تسهیل می‌کنند و شفافیت و مسئولیت‌پذیری را ارتقا می‌دهند. تولید استراتژیک محتوای دیجیتال معتبر به مقابله با اطلاعات نادرست و اطلاعات نادرست کمک می‌کند و به ثبات سیاسی کمک می‌کند. محتوای آموزشی در قالب‌های دیجیتال، سواد دیجیتال و توسعه مهارت‌ها را ارتقا می‌دهد و نیروی کار را برای اقتصاد دیجیتال آماده می‌کند. تولید محتوای دیجیتال از ابتکارات آموزش الکترونیکی پشتیبانی می‌کند و آموزش را در دسترس تر و فراگیرتر می‌کند. محتوای دیجیتال تعاملی و جذاب یادگیری مستمر و افزایش مهارت را تسهیل می‌کند و به جمعیتی آگاه و توانا کمک می‌کند. الزامات [illegible] محتوای دیجیتال باعث تحقیق و توسعه در زمینه‌هایی مانند هوش مصنوعی، واقعیت افزوده و واقعیت مجازی می‌شود. تلاقی تولید محتوا و فناوری، اکوسیستمی از نوآوری را تقویت می‌کند و توسعه ابزارها، پلتفرم‌ها و روش‌های جدید را تشویق می‌کند. نیاز به توزیع کارآمد محتوا منجر به پیشرفت در زیرساخت‌های دیجیتال، از جمله اینترنت پرسرعت و راه حل‌های ذخیره سازی داده‌ها می‌شود. تولید محتوای دیجیتال می‌تواند منجر به همکاری‌ها و مشارکت‌های بین المللی شود و نفوذ و شبکه‌های جهانی یک کشور را افزایش دهد. کشورها می‌توانند از طریق محتوای دیجیتال، ایجاد پل‌ها و تقویت درک متقابل با سایر کشورها، وارد دیپلماسی فرهنگی شوند. موفقیت کره جنوبی در تولید محتوای دیجیتال محبوب در سطح جهانی، مانند کی پاپ، درام‌ها و بازی‌ها، به طور قابل توجهی نفوذ فرهنگی و قدرت اقتصادی آن را افزایش داده است. ایالات متحده در تولید محتوای دیجیتال از طریق هالیوود، سیلیکون ولی و شرکت‌های رسانه‌ای مختلف پیشتاز است که قدرت نرم و قدرت اقتصادی آن را افزایش می‌دهد. چین به سرعت در حال گسترش صنعت محتوای دیجیتال خود با پلتفرم‌هایی مانند تیک تاک و سرمایه گذاری‌های قوی در بازی و فیلم است که حضور فرهنگی جهانی و رشد اقتصادی آن را تقویت می‌کند.

حکمرانی دیجیتال با ایجاد چارچوبی برای مدیریت، تنظیم و استفاده از فناوری‌ها و داده‌های دیجیتال، نقش مهمی در شکل‌دهی عمق ژئوپلیتیک دیجیتال یک کشور ایفا می‌کند. حکمرانی دیجیتال سیاست‌ها و مقرراتی را برای افزایش امنیت سایبری، حفاظت از زیرساخت‌های حیاتی و کاهش تهدیدات سایبری ایجاد می‌کند که شامل اقداماتی مانند قوانین امنیت سایبری، طرح‌های واکنش به حوادث و استانداردهای امنیت سایبری برای بخش‌های حیاتی است. حکمرانی دیجیتال موثر شامل مقرراتی است که از حریم خصوصی افراد محافظت می‌کند و بر جمع آوری، پردازش و به اشتراک گذاری داده‌ها نظارت می‌کند. این امر اعتماد به خدمات دیجیتال را افزایش می‌دهد و از داده ها مسئولانه و توسعه زیرساخت‌های دیجیتال قوی، از جمله شبکه‌های باند پهن، مراکز داده و خدمات ابری پشتیبانی می‌کند. این زیرساخت برای توانمندسازی نوآوری دیجیتال و رشد اقتصادی ضروری است. ارائه خدمات کارآمد و شفاف دولت الکترونیک را تسهیل می‌کند که شامل ابتکاراتی مانند سیستم‌های هویت دیجیتال، پورتال‌های خدمات آنلاین و رأی‌گیری الکترونیکی است که ارائه خدمات عمومی را بهبود می‌بخشد و مشارکت شهروندان را افزایش می‌دهد. محیطی مساعد را برای کارآفرینی و نوآوری دیجیتال ایجاد می‌کند؛ سیاست‌هایی که توسعه مهارت‌های دیجیتال، سرمایه‌گذاری در فناوری‌های دیجیتال و حمایت از استارت‌آپ‌ها و کسب‌وکارهای دیجیتال را ارتقا می‌دهد. هدف حکمرانی دیجیتال اطمینان از دسترسی همه شهروندان به فناوری‌ها و خدمات دیجیتال و از بین بردن شکاف دیجیتالی از طریق ابتکاراتی برای بهبود سواد دیجیتال، گسترش دسترسی پهنای باند و ترویج شنل دیجیتال برای گروه‌های به حاشیه رانده شده است. حکمرانی دیجیتال نقشی کلیدی در شکل دادن به تعامل بین المللی یک کشور در زمینه مسائل دیجیتال مثل مشارکت در مجامع بین المللی، مذاکرات در مورد قراردادهای تجارت دیجیتال و همکاری در زمینه امنیت سایبری و حفاظت از داده‌ها ایفا می‌کند. حکمرانی دیجیتال تضمین می‌کند که یک کشور بر زیرساخت‌ها و فناوری‌های دیجیتال خود از طریق اقداماتی برای محافظت در برابر مداخله خارجی، ترویج نوآوری داخلی و تاکید بر حاکمیت در فضای سایبری کنترل دارد.

مقدمه

پیشرفت‌های عظیم فناوری بر روند تغییرات اجتماعی، سیاسی و اقتصادی کشورها تأثیر گذاشته است. تکنولوژی به سرعت در حال تحول است که بر سیستم‌های اجتماعی، سیاسی و اقتصادی نیز تأثیر می‌گذارد. تقریباً هر جنبه‌ای از زندگی انسان در اینترنت به هم مرتبط شده است. فناوری به پایه زندگی اجتماعی بشر تبدیل شده است. نمی‌توان انکار کرد که مسائل ژئوپلیتیک به عنوان یکی از حوزه‌های مطالعات روابط بین الملل به جریان تغییرات تکنولوژیک نیز کشیده شده است. مطالعات ژئوپلیتیک به عنوان یکی از مطالعاتی که به بررسی تعامل بین پویایی سیاسی و جغرافیا می‌پردازد، در معرض پیامدهای تحولات فناوری قرار می‌گیرد. در مطالعات ژئوپلیتیکی اولیه استراتژی‌ها و سیاست‌های دولت برای به دست آوردن نفوذ در مناطق خاص مورد بحث قرار می‌گرفت؛ مثلا ژئوپلیتیک به معنای مطالعه مرزهای یک کشور. ظهور فضای دیجیتال در کنار پیشرفت فناوری، پیامدهایی برای توسعه ژئوپلیتیکی یک کشور دارد. در نتیجه رقابت ژئوپلیتیکی نه تنها در عرصه فیزیکی، بلکه در فضای دیجیتال نیز صورت می‌گیرد. ژئوپلیتیک فضای دیجیتال مرز ندارد. برای جلوگیری از درگیری‌های سایبری، دولت‌ها باید فضای سایبری را حوزه سیاسی خود قرار دهند. رقابت‌های ژئوپلیتیکی بین دولت‌ها در فضای دیجیتال می‌تواند پیامدهای واقعی داشته باشد. یکی از آنها استفاده از فناوری برای سرکوب سیاست‌های ژئوپلیتیکی دولت‌های دیگر است. از آنجایی که فضای مجازی بی نهایت است، دولت باید حکمرانی خود را در آن توسعه دهد تا درگیری‌های سایبری احتمالی عواقب فیزیکی برای ژئوپلیتیک کشور نداشته باشد. با توجه به اینکه تقریباً تمام پویایی‌های زندگی دولتی در فناوری اطلاعات ادغام شده‌اند، فضای دیجیتال را باید یکی از حوزه‌های ژئوپلیتیکی دولت‌ها در نظر گرفت.

ژئوپلیتیک از بحث در مورد رابطه بین انسان و جغرافیای منطقه متولد شد. همان طور که فرهنگ بشری تکامل می‌یابد، جغرافیا به یک شاخص مهم از توانایی یک جامعه برای توسعه توانایی‌های خود تبدیل می‌شود (O Tuathail, 1996). هالفورد جی. مکیندر، پیشگام در مطالعات ژئوپلیتیک، موقعیت جغرافیایی را با امکان توسعه قدرت یک دولت توضیح داد. این را می‌توان در توسعه نظریه هارتلند مکیندر مشاهده کرد، که ادعا می‌کند دولتی که بتواند جزیره جهان (منطقه اوراسیا) را کنترل کند می‌تواند کل جهان را کنترل کند (مکیندر، ۱۹۹۸). اما این نظریه به دلیل اینکه بیش از حد غرب

محور و امپریالیستی بود رد شد(Power, 2010). علاوه بر این، نظریه ژئوپلیتیک کلاسیک بر قوم گرایی، مرد محوری و به حاشیه راندن کشورهای غیر غربی تأکید دارد.

مطالعات ژئوپلیتیک به شاخصی برای تقسیم جهانی بلوک غرب و اتحاد جماهیر شوروی در طول جنگ سرد تبدیل شد. وینستون چرچیل در یک سخنرانی در پایان دهه ۱۹۴۰ میلادی تاکید کرد که قلمروی که در بلوک شرق گنجانده شده است بخشی از پرده آهنین است. در آن زمان، ژئوپلیتیک مترادف با ابرقدرت‌هایی بود که قلمروهای جهان را به منظور به دست آوردن مزیت‌های سیاسی و نظامی کنترل می‌کردند(Dodds, 2007). علاوه بر این، ژئوپلیتیک همیشه با چگونگی تأثیر مستقیم عناصر جغرافیایی بر زندگی سیاسی یک دولت مرتبط است. محققان ژئوپلیتیک می‌توانند با درک مفهوم جغرافیا، چگونگی تأثیر تعاملات اقتصادی، سیاسی و اجتماعی بر جهت گیری سیاست‌ها را تفسیر کنند. مطالعات ژئوپلیتیک به یک بینش یا جهت گیری برای دولت تبدیل می‌شود تا سیاست خارجی خود را در سطح اجرا تنظیم کند. به عنوان مثال، در مطالعات ژئوپلیتیک، مفهوم مکان به عنوان ویژگی‌های یک مکان که با مفهوم محلی (محل) همبستگی دارد، تعریف می‌شود. محلی به عنوان یک نهاد اجتماعی-سیاسی جامعه در یک منطقه جغرافیایی خاص. مثلا سیستم اجتماعی و شکل حکومت یک جامعه دریایی با جامعه کشاورزی متفاوت خواهد بود زیرا سبک زندگی آن‌ها تحت تأثیر شرایط جغرافیایی که در آن زندگی می‌کنند است(فلینت، ۲۰۱۶). ژئوپلیتیک چیزی فراتر از نحوه ساماندهی یک دولت در یک منطقه است. علاوه بر این، ژئوپلیتیک مزایای سیاسی توسعه همکاری دولتی بین مناطق را مورد بحث قرار می‌دهد(پاور، ۲۰۱۰). علاوه بر این .ژئوپلیتیک جمعیت و جریان حرکت انسان و همچنین پیامدهای آن برای مناطقی که در آن زندگی می‌کنند را بررسی می‌کند(مرچنت، ۲۰۱۵).

تعاریف متعددی برای اصطلاح ژئوپلیتیک ارائه شده است. کالین فلینت ژئوپلیتیک را به عنوان مطالعه‌ای تعریف می‌کند که ویژگی‌های یک منطقه را با پویایی سیاسی آن مرتبط می‌کند(فلینت، ۲۰۱۶). به عقیده فلینت، یک نهاد ژئوپلیتیکی مانند یک دولت به توانایی دفاع از مناطق مسکونی یا گسترش مناطق فراتر از مرزهای خود نیاز دارد(فلینت، ۲۰۱۶). به زعم دادز، این تعریف فلینت در دوران جنگ سرد به شکل توازن قوا بین دو قدرت بزرگ که برای تسلط بر مناطق جهانی می‌جنگیدند، دیده شد.(Dodds, 2007) سائول بی کوهن، برخلاف مفروضات فلینت، ژئوپلیتیک

را به عنوان یک قانون اساسی علمی که به مدیریت سرزمین‌ها از طریق دکترین سیاسی مربوط می‌شود، تعریف کرد. به عقیده کوهن، ژئوپلیتیک چیزی نیست جز رقابت بین کشورها برای به دست آوردن نفوذ در یک منطقه با در نظر گرفتن جغرافیای انسانی و علوم سیاسی کاربردی. کوهن ژئوپلیتیک را به عنوان فرآیند تعامل سیاست با نظم جغرافیایی تعریف کرد. تعریف ژئوپلیتیک کوهن به بسیاری از ایده‌های ژئوپلیتیک کلاسیک از جمله ایده‌های هاوسهوفر، مکیندر، اسپایکمن و ماهان اشاره دارد(کوهن، ۲۰۱۵). ژئوپلیتیک را نمی‌توان از نقش دولت در دستیابی به قدرت برای تبدیل شدن به هژمون در یک منطقه در سطح اجرای سیاسی جدا کرد. ژنگیو وو در تحقیقات خود توضیح داد که در چارچوب ژئوپلیتیک کلاسیک، دولت با ایجاد تعادل در قدرت رقابت می‌کرد. دولت به دنبال تسلط و اعمال نفوذ بر زمین، دریا، هوا و سایر مناطق استراتژیک مانند هارتلند از طریق توازن قدرت بوده است(Wu, 2018).

اما پس از پایان جنگ سرد، کارشناسان روابط بین الملل شروع به زیر سوال بردن تعریف ژئوپلیتیک کردند؛ به ویژه تعاریفی که قاطعانه حامی امپریالیسم و برتری سفیدپوستان است O) .(Tuathail, 1996اوتوتایتل در کتاب خود با عنوان ژئوپلیتیک انتقادی تعریف ژئوپلیتیک را که بر جنبه قدرت سخت تأکید دارد، زیر سوال می‌برد. وی همچنین بر اهمیت تعریف اصطلاحات ژئوپلیتیک با عناصر غیرسیاسی مانند هویت، نژاد، جنسیت و حتی مذهب تاکید می‌کند. جنیفر هیندمن، شخصیت‌های منتقد ژئوپلیتیک، بیان کرده است که تعریف فعلی ژئوپلیتیک مترادف با جنگ و خشونت است. او ادعا می‌کند که درگیری‌های ناشی از گسترش ژئوپلیتیکی یک کشور، اغلب بر رنج غیرنظامیان مانند زنان و کودکان سرپوش می‌گذارد(جونز و سیج، ۲۰۱۰). محققان ژئوپلیتیکی مانند دبورا کوون و نیل اسمیت با ساختارشکنی تعریف ژئوپلیتیکی آن را مملو از ظرایف استعماری یافتند، اصطلاح جدیدی به نام ژئوپلیتیک اجتماعی را برای توصیف مطالعه تعامل بین انسان‌ها و جغرافیا، از جمله جنبه‌های سیاسی و همچنین تعاملات اجتماعی و اقتصادی ابداع کردند (Cowen & Smith, 2009). کوئن و اسمیت تعریف ژئوپلیتیکی از نفوذ ایالات متحده را که سایر بازیگران ژئوپلیتیک را نادیده می‌گرفت، رد کردند. با این حال، آنها مفاهیم فضا، قدرت و امنیت را می‌پذیرند. آنها می‌خواهند مفهوم ژئوپلیتیک عاری از عناصر استعمار منطقه‌ای باشد.

اکنون بحث مسائل ژئوپلیتیک از حوزه فیزیکی به فضای مجازی منتقل شده است و فضای

مجازی به یکی از مهم ترین حوزه‌های ژئوپلیتیک تبدیل شده است. شلدون (۲۰۱۴) تغییر مسائل ژئوپلیتیکی را در نتیجه اولویت دادن کشورها به فضای سایبری به عنوان بخشی از قلمرو خود توصیف نموده است. از سوی دیگر شلدون معتقد است که جدای از دنیای مجازی نامرئی، درگیری در قلمرو مجازی پیامدهایی در قلمرو فیزیکی دارد. اکنون باید مسائل ژئوپلیتیک را نه تنها به صورت فیزیکی، بلکه دیجیتالی نیز تفسیر کرد. ژئوپلیتیک دیگر از رابطه بین مناطق، سیاست و ابزارهای اقتصادی در توسعه سرمایه گذاری منطقه‌ای بحث نمی‌کند. هرچند همچنان تسلط و کنترل بر منابع طبیعی برای دستیابی به منافع ژئوپلیتیکی یک کشور از موضوعاتی است که در مطالعات ژئوپلیتیک به آن پرداخته می‌شود و رقابت ژئوپلیتیکی و رقابت برای تبدیل شدن به هژمون در یک منطقه، همچنان نقش مهمی در مطالعات ژئوپلیتیک ایفا می‌کند.

طبق گزارشی که توسط کاوش (۲۰۱۷) گردآوری شده است، درگیری‌های سایبری پیامدهایی بر ثبات ژئوپلیتیکی یک دولت دارد. کاوش در مطالعه موردی خود اظهار داشت که ثبات ژئوپلیتیکی نه تنها به روابط فیزیکی بین کشورها، بلکه به روابط سایبری نیز وابسته است. او حمله استاکس‌نت به برنامه غنی‌سازی ایران توسط هکرهایی اسرائیلی(فلسطین اشغالی) را نمونه‌ای از پیچیده‌تر شدن روابط کشورها عنوان کرد (کاوش، ۲۰۱۷). بر اساس گزارش پابلیک پرایوت[1] (۲۰۱۹) نوسانات ژئوپلیتیکی یک منطقه در قلمرو سایبری می‌تواند باعث نابسامانی گردد. طبق این گزارش بازیگران نوظهور و بازیگران فرصت‌طلب، می‌توانند تهدیدی برای ثبات ژئوپلیتیکی در قلمرو سایبری باشند. بازیگران نوظهور، بازیگران دولتی، گروه‌های تروریستی و سازمان‌های جنایتکاری هستند که قادر به سازماندهی و انجام حملات سایبری به شیوه‌ای ساختاریافته و سازمان یافته هستند.

فضای دیجیتال شبکه‌ای از فعالیت‌های دیجیتالی است که فضای فیزیکی و فضای مجازی را به هم متصل می‌کند. به نظر ریوردان، فضای مجازی با سیاست‌های ژئوپلیتیک یک کشور پیوند دارد. تمام فعالیت‌های انسانی که به آنها «حوزه‌های انسانی» گفته می‌شود، در فضای مجازی حضور دارند. این حوزه فعالیت‌های انسانی را به فناوری فضای سایبری متصل می‌کند و با منافع ژئوپلیتیکی یک کشور در ارتباط است(ریوردان، ۲۰۱۹). مارتین دوج و راب کیچن در کتاب نقشه برداری فضای

1 . Public Private (2019)

مجازی، فضای مجازی را به عنوان جغرافیای یک جامعه اطلاعاتی تعریف می‌کنند. این تعریف با محتوای متنوع فضای مجازی پیوند دارد. در هر دقیقه، میلیون‌ها فعالیت دیجیتالی در فضای مجازی انجام می‌شود(دوج و کیچین، ۲۰۰۱). فضای مجازی اغلب با منافع ژئوپلیتیکی یک کشور تلاقی می‌یابد. فضای مجازی عاری از مرزهای سرزمینی است. با این حال، فضای مجازی باعث ایجاد تغییری می‌شود که به عنوان «فرهنگ جهانی» شناخته می‌شود. تبادل اطلاعات سیاسی، اقتصادی و فرهنگی دولت را وادار می‌کند تا محدوده منافع خود را در فضای سایبری ترسیم کند. راه دیگر برای تعریف فضای مجازی به عنوان یک دامنه جهانی با شبکه‌هایی است که سخت افزار، نرم افزار و بسته‌های داده را به هم متصل می‌کنند. فضای مجازی باید از نظر فنی دارای سه لایه باشد: سخت افزار(کامپیوتر، مدارهای کابلی، زیرساخت فناوری اطلاعات)، نرم افزار (برنامه‌های عملیاتی) و بسته‌های داده(تساگوریاس، ۲۰۱۵). فضای سایبری به عنوان قلمروی مستقل توضیح می‌دهد که چگونه دولت می‌تواند اقتدار خود را کنترل و اعمال کند به همان شیوه‌ای که از فضای فیزیکی برای مشروعیت بخشیدن به سیاست استفاده می‌کند(تساگوریاس، ۲۰۱۵).

تعاملات دولتی در فضای مجازی پیامدهای فیزیکی غیرمستقیم ژئوپلیتیکی دارد. علاوه بر این، سایبر یکی از ابزارهای ژئواکونومیکی است که دولت می‌تواند از آن برای دستیابی به اهداف ژئوپلیتیکی خود استفاده کند(Blackwill & Harris, 2017). [illegible] دولت‌ها در ژئوپلیتیک دیجیتال این است که فضای سایبری منطقه‌ای بدون مرز است در نتیجه، ثبات ژئوپلیتیکی یک کشور در حوزه سایبری باید در نظر بگیرد که چه نوع حکومتی می‌تواند منافع امنیتی خود را در دنیای بدون مرز حفظ کند. توجه به قلمرو سایبری توسط دولت قابل اجتناب نیست. در نتیجه کشورها باید به همان اندازه که به حوزه‌های فیزیکی توجه می‌کنند به این حوزه‌ها نیز توجه کنند.

از نظر ران دیبرت[1] معادلات ژئوپلیتیک در فضای مجازی پس از ماجرای ادوارد اسنودن[2] به طرز چشمگیری تغییر کرد. دیبرت در پژوهش خود توضیح می‌دهد که چگونه نقش دولت ایالات متحده در اجرای سیاست‌های پرایسم[3] می‌تواند ثبات ژئوپلیتیکی کشورهای دیگر مناطق را مختل

1 . Ron Deibert

2 . Edward Joseph Snowden

۳ . ادوارد اسنودن در سال ۲۰۱۳، اسنادی را از آژانس امنیت ملی امریکا فاش کرد که نشان از وجود دو برنامه نظارتی دولت امریکا داشت: PRISM و UPSTREAM. که هر دو ذیل بخش ۷۰۲ (section702) قانون نظارت بر اطلاعات خارجی(FISA) به روش‌های مختلف کار می‌کردند: پرایسم شامل جمع آوری مستقیم ارتباطات در پایین دست توسط آژانس امنیت ملی از طریق

کند(Deibert, 2015). در نتیجه حادثه اسنودن، کشورهای عضو اتحادیه اروپا سیاست‌های جداگانه‌ای برای حفاظت از منافع ژئوپلیتیکی خود در برابر جاسوسی برای دولت ایالات متحده اتخاذ کردند(دیبرت، ۲۰۱۵).

ریوردان به موقعیت ایالات متحده به عنوان هژمون در فناوری می‌پردازد. با توجه به وضعیت فعلی ایالات متحده در جهان، سیاست‌های آن در فضای مجازی نیز قابل درک است. فعالیت‌های آن را می‌توان به تلاش‌های دولت این کشور برای نظارت بر فعالیت‌های اینترنتی در سراسر جهان از طریق آژانس امنیت ملی ردیابی کرد(Riordan, 2019). به نظر می‌رسد که این سیاست نشان دهنده حضور ژئوپلیتیکی ایالات متحده، هم به صورت فیزیکی و هم مجازی است. نفوذ ژئوپلیتیک ایالات متحده به صورت فیزیکی در تمام مناطق جهان قابل مشاهده است. چیزی که ایالات متحده آرزوی دستیابی به آن را دارد این است که نفوذ آن‌ها حتی در فضایی بدون مرز احساس شود. روس‌ها هم از نظر ژئوپلیتیکی سعی کردند نفوذ خود را در کشورهای اتحاد جماهیر شوروی سابق حفظ کنند. به عنوان مثال، روسیه حملات سایبری متعددی را به زیرساخت‌های حیاتی در اوکراین، گرجستان و استونی انجام داده است. روسیه این حملات سایبری را به عنوان نوعی اعتراض پس از شکست در دستیابی به توافق روابط دوجانبه با این کشورها انجام داد. این حمله سایبری بر برتری قاطع روسیه تاکید کرد و به نماد برتری این کشور تبدیل شد .(Riordan, 2019) در همین حال، چین از دیدگاه ژئوپلیتیک، در تلاش است مستقل از نفوذ غرب باشد (ریوردان، ۲۰۱۹). به عنوان مثال، پروژه دیوار آتش بزرگ چین [1] بر این نکته تاکید دارد که این کشور به دنبال محافظت از منافع سایبری خود مستقل از هر بازیگری است. این سیاست نشان دهنده گامی به سوی استقلال فناوری چین از کشورهای غربی است.

شلدون توضیح می‌دهد که چگونه درگیری سایبری بر منافع ژئوپلیتیک فیزیکی دولت تأثیر می‌گذارد. شلدون در یکی از تحلیل‌های خود توضیح داد که یک دولت با حملات سایبری بر مناطق تحت نفوذ خود تأثیر می‌گذارد. به عنوان مثال، حمله سایبری به راکتور هسته‌ای ایران در نطنز، نوعی

کمک اجباری ارائه دهندگان خدمات ارتباطات الکترونیکی است. به این صورت که دولت یک خدمت ارتباطات الکترونیکی مانند یک آدرس ایمیل متعلق به یک فرد یا سازمان و یا دولت را به یک ارائه دهنده خدمات ارتباطات الکترونیکی مستقر در ایالات متحده می‌فرستد و ارائه دهنده موظف است تمام ارتباطات ارسال شده به یا از آن را در اختیار دولت قرار دهد.

1 . Great Firewall

اختلال از سوی مخالفان سیاسی ایران به منظور جلوگیری از تبدیل شدن ایران به یک هژمون در خاورمیانه است. مورد دیگر، استفاده چین از جاسوسی سایبری برای سرقت فناوری از کشورهای توسعه یافته مانند اروپا و ایالات متحده است. چین در تلاش است تا فناوری داخلی را توسعه دهد و در عین حال از طریق این فعالیت‌های جاسوسی از نفوذ غرب جدا شود. با این استقلال تکنولوژیکی، چین به دنبال اثبات این است که بازیگری کلیدی در چشم انداز ژئوپلیتیک جهانی، هم از نظر فیزیکی و هم مجازی است. شلدون همچنین امکان درگیری سایبری و تأثیر آن بر ادغام فناوری اطلاعات و ارتباطات و دستگاه‌های فیزیکی مختلف متصل به شبکه اینترنت اشیاء توسط بسیاری از کشورها را مورد بحث قرار داد(شلدون، ۲۰۱۴). این مطالعه در توضیح تغییر پارادایم از ژئوپلیتیک فیزیکی به فضای سایبری و درگیری‌های احتمالی آینده صادق است. به گفته بلک ویل و هریس، فناوری اطلاعات کل زندگی اجتماعی، سیاسی و اقتصادی کشورها را یکپارچه کرده است. آن‌ها توضیح دادند که چگونه دولت می‌تواند از فناوری برای پیشبرد منافع ژئوپلیتیکی خود استفاده کند. بلک ویل و هریس به عنوان مثال، استدلال می‌کنند که یک حمله سایبری برنامه ریزی شده به زیرساخت‌های دولتی، ثبات دولت و منطقه را خدشه دار می‌اندازد.

رقابت بین ایران، عربستان سعودی و رژیم صهیونیستی (فلسطین اشغالی) نمونه رقابت ژئوپلیتیکی در هر دو حوزه فیزیکی و سایبری است (کاوش، ۲۰۱۷). حمله سایبری به رآکتور هسته‌ای ایران دلیلی تجربی بر عدم تمایل رژیم اشغالگر صهیونیستی به تلقی ایران به عنوان یک قدرت ژئوپلیتیکی مهم در خاورمیانه است(شلدون، ۲۰۱۴). در چشم انداز ژئوپلیتیک خاورمیانه، ایران با رژیم صهیونیستی(فلسطین اشغالی) و عربستان سعودی رقابت دارد. در همین حال، سیاست خارجی ایران اغلب با سیاست آمریکا و متحدانش در تضاد است. ایران و عربستان سعودی برای تبدیل شدن به هژمون در رقابت ژئوپلیتیکی خاورمیانه با یکدیگر رقابت می‌کنند(رمضان و اسکندر، ۲۰۲۰). از سوی دیگر، درگیری‌های دولتی در فضای سایبری پیامدهایی برای ثبات ژئوپلیتیکی در حوزه فیزیکی دارد. جدا از مثال‌های ذکر شده فوق، ژئوپلیتیک در درجه اول یک فلسفه و یک دیدگاه دولتی است(کلی، ۲۰۰۶). به گفته اتوتایتل، ژئوپلیتیک فلسفه‌ای است که گاهی برای مشروعیت بخشیدن به دولت‌های توسعه طلب به کار می‌رود. جغرافیا یا قلمرو به اشیایی که با چشم غیر مسلح قابل مشاهده است محدود نمی‌شود. به طور خاص، اتوتایتل تأکید کرد که جغرافیا برای یک کشور

توسعه‌طلب رسانه‌ای است که برای گسترش ارتباطات یا تسهیل تدارکات جنگ استفاده می‌شود. بر اساس دیدگاه اوتاتیل، امکان درگیری و رقابت ژئوپلیتیکی هم در حوزه فیزیکی و هم در فضای مجازی وجود دارد. فضای مجازی به دلیل ماهیت بدون مرز خود، مرزهای فیزیکی را که معمولاً در داخل مرزهای یک کشور دیده می‌شود، محو می‌کند. فقدان مرزهای فیزیکی احتمال درگیری ژئوپلیتیکی یک دولت را پیچیده می‌کند. وجود حاکمیت دولت را قادر می‌سازد تا قلمرو خود را به طور مستقل اداره کند. اما این موضوع در فضای مجازی صدق نمی‌کند. برخلاف توافقنامه وستفالن در سال ۱۶۴۸ میلادی این دولت دیگر مرزهای سرزمینی را به رسمیت نمی‌شناسد(Mueller, 2019). زمانی که یک کشور برای دستیابی به منافع ژئوپلیتیکی خود باید درگیر منازعه در فضای سایبری شود، راه حل مسالمت آمیز دشوارتر می‌شود. کاربران می‌توانند به صورت ناشناس در فضای مجازی به اینترنت دسترسی داشته باشند. این تابع ناشناس در نهایت منجر به درگیری‌های نامتقارن می‌شود.

اما نکته‌ای که باید در نظر داشت این است که ساختار ژئوپلیتیکی به سه بخش تقسیم می‌شود؛ «قلمرو ژئواستراتژیک»، «منطقه ژئوپلیتیک» و «دولت‌های ملی»(کوهن، ۲۰۱۵). کوهن معتقد است که دولت برای حفظ ثبات ژئوپلیتیکی، چه در سطح منطقه و چه در سطح جهانی، حیاتی است. در زمینه ژئوپلیتیک فضای مجازی، دولت در مدیریت تمام ابعاد حیات خود در مواجهه با تهدیدات مختلف که پتانسیل برهم زدن ثبات ژئوپلیتیکی را دارد، نیازمند نقش ویژه است.

تهدیدات در فضای سایبری به دو دسته ساختاریافته یا بدون ساختار طبقه بندی می‌شوند. تهدیدهای ساختاریافته پیامدهای بلندمدت و قابل پیش بینی دارند که می‌توانند ثبات ژئوپلیتیکی را بی ثبات کنند. حملات سایبری ساختاریافته معمولاً توسط متخصصان و سازمان‌هایی مانند دولت‌ها، سازمان‌های جنایتکار یا سازمان‌های تروریستی برنامه‌ریزی می‌شوند. در همین حال، حملات بدون ساختار پراکنده هستند و کوتاه مدت هستند و با استفاده از نفوذ غیرقانونی برای تغییر ظاهر سایت‌های اینترنتی مشخص می‌شود(Dunn Cavelty, 2010). علاوه بر این، دولت باید از خود در برابر اختلالات ژئوپلیتیکی در فضای سایبری محافظت کند. برخی از کارشناسان حتی پیشنهاد می‌کنند که فضای مجازی بومی سازی شود. وستفالیایی شدن در درجه اول با ترویج ایجاد مرزهای دولتی در فضای سایبری مرتبط است. اکنون فضای مجازی به عنوان یک فضای مشترک شناخته می‌شود که نمی‌تواند در محدوده‌های ژئوپلیتیکی قرار گیرد (کورنیش، ۲۰۱۵). با این حال، برای جلوگیری

از انواع مختلف اختلالات ژئوپلیتیکی، چندین کشور شروع به گنجاندن فضای سایبری به عنوان بخشی از حاکمیت خود کرده اند(شن، ۲۰۱۶). بدون شک دولت باید برای مقابله با هر نوع اختلال در فضای مجازی آماده باشد. کشورها به همان شیوه‌ای که در حوزه فیزیکی تعامل دارند، یعنی از طریق درگیری و همکاری، در فضای مجازی هم تعامل دارند. کشورها می‌توانند از استراتژی «خودیاری» مکتب واقع‌گرایی استفاده کنند. در این زمینه، کشورها می‌توانند قابلیت‌های تکنولوژیکی خود را برای محافظت از خود در برابر حملات سایبری سایر کشورها ارتقا دهند. در نتیجه، کشورها باید قابلیت‌های منابع انسانی و نوآوری‌های فناوری را توسعه دهند تا بتوانند در فضای سایبری رقابت کنند (رمضان، ۲۰۱۹).

استراتژی‌های بازدارندگی می‌تواند توسط کشورهای دارای فناوری پیشرفته برای جلوگیری از تهدیدات سایر کشورها مورد استفاده قرار گیرد(کساب، ۲۰۱۴). در طول جنگ سرد، استراتژی‌های بازدارندگی در مطالعات ژئوپلیتیک رایج بود. تقسیم‌بندی ناتو و پیمان ورشو در جغرافیای سیاسی اروپا، شواهد ملموسی از رقابت‌های بازدارنده ابرقدرت‌ها است(کوهن، ۲۰۱۵). الگوی بازدارندگی به سبک جنگ سرد می‌تواند در حوزه سایبری برای پیروزی در رقابت فضای سایبری و ژئوپلیتیکی مورد استفاده قرار گیرد. راهبردهای بازدارندگی را می‌توان با توسعه فناوری عملی به اجرا گذاشت. هدف همانند حوزه فیزیکی است؛ بازدارندگی از مخالفان سیاسی (کساب، ۲۰۱۴). این الگوی «خودیاری» به شدت تحت تأثیر دولت است. در نتیجه، تلاش‌های دولت برای برنده شدن در رقابت‌های ژئوپلیتیکی در فضای سایبری بایستی بر حداکثر کردن قدرت نظامی، اقتصادی و فناوری متمرکز باشد (ایسنارتی، ۲۰۱۶).به عنوان مثال تعهد دولت چین به مستقل ساختن کشورش از نظر تکنولوژیکی و مستقل از سایر کشورها، نمونه بارز اجرای سیاست«خودیاری» است(ریوردان، ۲۰۱۹). دولت چین به طور کامل اهمیت حق حاکمیت اینترنت در دفاع از قلمرو فضای سایبری خود را به رسمیت می‌شناسد. جاسوسی سایبری، جرایم سایبری و جنگ سایبری همگی تهدیدهای وحشتناکی برای منافع ملی چین هستند. دلیل این امر به طور جدایی ناپذیری با حادثه اسنودن مرتبط است. برای اطمینان از اینکه منافع ژئوپلیتیک چین به خطر نمی‌افتد، دولت شی جین پینگ مدرن سازی را در فضای سایبری اجرا کند .(Zeng et al., 2017) دولت چین با سیاست «دیوار آتش بزرگ چین» کشور را به خودکفایی در زمینه فناوری رهنمون می‌کند. آنها تشخیص دادند که

فناوری می‌تواند به عنوان یک ابزار سیاسی برای خنثی کردن سیاست‌های یک کشور مورد استفاده قرار گیرد (ریوردان، ۲۰۱۹).

به عقیده بوزان و ویور، ثبات ژئوپلیتیکی یک منطقه را می‌توان در الگوهای «دوستی» و «دشمنی» در میان کشورهای منطقه مشاهده کرد. اگر الگوهای تعامل کشورها خصمانه باشد، وضعیت ژئوپلیتیکی در منطقه احتمالاً متخاصم خواهد بود. برعکس، اگر الگوی تعامل دوستانه باشد، مشارکت و همکاری غالب‌تر است (Buzan & Weaver, 2003). علاوه بر این، ناوری توضیح داد که مشکلات همه دولت‌ها غالبا یکسان است. با این حال، همه کشورها قادر به حل مشکلات نیستند. تعاملات مشترک بین کشورها بعضا می‌تواند به حل این مشکلات کمک کند (ناوری، ۱۳۹۲). به طور کلی لیبرالیسم معتقد است که مشکلات ژئوپلیتیکی و فضای مجازی دولت تنها با همکاری قابل حل است. یک مثال تجربی، همکاری امنیت سایبری آغاز شده توسط آسه آن در جنوب شرقی آسیا است که هدف آن حفظ ثبات ژئوپلیتیکی و ژئواکونومیکی است- (رمضان، ۲۰۲۰). دشمن این حالش در حفظ ثبات ژئوپلیتیکی و ژئواکونومیکی آنها، توسعه هنجارها و قوانین امنیت سایبری است که بتواند همه کشورهای عضو اعمال شود. آسیای جنوب شرقی بدون شک به یک منطقه یکپارچه اقتصادی و سیاسی تبدیل شده است. برای حفظ این ثبات، آسه آن متعهد به تضمین امنیت فضای سایبری خود است که پیامدهایی بر وضعیت ژئوپلیتیک آسیای جنوب شرقی دارد (رمضان، ۲۰۱۷). علاوه بر این، آسه آن در حفاظت از زیرساخت‌های حیاتی خود در برابر حملات سایبری و خرابکاران فراملی و گروه‌های تروریستی و سازمان‌های جنایتکار بین المللی با چالش‌هایی مواجه است (Neubert, 2017). در همین حال، در منطقه اوراسیا، کشورهایی مانند روسیه، چین و کشورهای آسیای مرکزی برای حفظ ثبات ژئوپلیتیکی در فضای سایبری با یکدیگر همکاری می‌کنند. کشورهای منطقه یک کد رفتاری را ایجاد کرده‌اند که به نام «آیین رفتار بین المللی برای امنیت اطلاعات» شناخته می‌شود (آساف و همکاران، ۲۰۲۰). این ائتلاف به این دلیل تشکیل شد که روسیه، چین و کشورهای آسیای مرکزی دارای منافع ژئوپلیتیکی و ژئواکونومیکی به ویژه در زمینه اکتشاف گاز هستند. این کشورها عضو «سازمان شانگهای» هستند که به سازمان همکاری شانگهای نیز معروف است.

صرف‌نظر از سیاست‌های دولت در اجرای استراتژی‌های درگیری یا رقابت، حاکمیت فضای سایبری همچنان مورد نیاز است. موقعیت ژئوپلیتیکی یک کشور در فضای سایبری نیز ادامه دارد (فرناندز، ۲۰۲۰). تلاش‌ها برای گنجاندن فضای مجازی در حوزه ژئوپلیتیکی ادامه دارد. با این حال، فضای مجازی یک

فضای عمومی بسیار به هم پیوسته است که در نتیجه این وضعیت، خطوط اقتدار دولتی در فضای مجازی به طور فزاینده‌ای مبهم می‌شود(تساگوریاس، ۲۰۱۵). همان طوری که گفته شد یک گام مهم در تحلیل سیاست‌های ژئوپلیتیکی یک کشور در فضای مجازی، بومی‌سازی یا وستفالی‌سازی اقتدار دولتی در فضای مجازی است. دولت ترکیه همان کاری را کرد که دولت چین با بومی کردن فضای مجازی انجام داد. دولت ترکیه در حال توسعه یک مدل سیاست امنیتی فضای سایبری از طریق وزارت حمل و نقل و زیرساخت است تا از زیرساخت‌های حیاتی خود محافظت کند (Eldem, 2020) . گذشته از حوزه عمومی فضای مجازی، دولت این اختیار را دارد که از منافع ژئوپلیتیکی خود در فضای سایبری محافظت کند(Khanna, 2018). وقتی امنیت دولت‌ها در فضای مجازی به خطر می‌افتد، صلاحیت دفاع از منافع خود را دارند. در نتیجه، دولت باید یک مقررات استاندارد امنیتی فضای سایبری داشته باشد تا اختلالی در ثبات ژئوپلیتیکی نداشته باشد. در حال حاضر اکثر دولت‌ها در رتبه دولت‌های با فناوری بالا طبقه بندی می‌شوند. این بدان معناست که اکثر کشورها برای ترکیب مدل دولتی به سبک وستفالیا با پیچیدگی تکنولوژیک تطابق یافته‌اند. در این مرحله، فناوری ستون فقرات عملیات دولت است(اشپیگل، ۲۰۰۰). کشورها باید اقتدار خود را در فضای سایبری نشان دهند و به طور طبیعی توانایی‌های تکنولوژیکی خود را ارتقا دهند. از این گذشته، فناوری می‌تواند به عنوان یک ابزار سیاسی برای سرکوب موقعیت‌های ژئوپلیتیکی و همچنین رسانه‌ای رقبا برای متعادل کردن قدرت دولت‌ها مورد استفاده قرار گیرد (دان کاولتی و ونگر، ۲۰۲۰). در ژئوپلیتیک، وجود حاکمیت فضای سایبری فرآیندی است که همه ذینفعان را گرد هم می‌آورد تا مکانیزمی برای تدوین سیاست‌های مرتبط با موضوعات خاص تشکیل دهند. با توجه به ماهیت بسیار ناهمگون فضای مجازی، چنین حکمرانی باید فرابخشی باشد. کارول ام. گلن اظهار داشت که این اصول حکمرانی باید بر اساس منافع دولت، سازمان‌های بین‌المللی، کسب‌وکارها و جامعه مدنی ساخته شوند(گلن، ۲۰۱۴).

با این حال، به نظر می‌رسد که درگیری بر سر مرزهای سیاست دولتی در فضای مجازی موضوع جدیدی است. به ویژه حمایت انسانگرایان که می‌خواهند فضای مجازی به عنوان منطقه میراث مشترک بشریت تعیین شود. از این نظر این منطقه باید عاری از ادعای حاکمیت باشد و هرگونه نفوذ و فعالیت ژئوپلیتیکی که در آنجا انجام می‌شود باید بر اساس صلح و رفاه برای بشریت باشد(Klinger, 2020). با این وجود، ضرورت حکمرانی فضای مجازی برای حفظ یکپارچگی ژئوپلیتیکی کشور، منطقه و جهانی

را نمی‌توان رد کرد. حاکمیت فضای سایبری، مانند آنچه که توسط گروه کارشناسان دولتی سازمان ملل متحد [1] ارائه شده است، لازم است تا اطمینان حاصل شود که دولت‌ها با بی احتیاطی از فناوری سوء استفاده نمی‌کنند (کورن و تیلور، ۲۰۱۷). طبق اعلامیه گروه کارشناسان دولتی امنیت اطلاعات سازمان ملل متحد، حاکمیت سایبری باید تعادلی بین حاکمیت دولت و قوانین بین‌المللی ایجاد کند (کورن و تیلور، ۲۰۱۷). علاوه بر گروه کارشناسان دولتی امنیت اطلاعات سازمان ملل متحد، کشورها می‌توانند قوانین رفتاری راهنمای تالین [2] را برای فعالیت‌های دولتی در فضای سایبری اتخاذ کنند. بر اساس این دستورالعمل، نفوذ غیرقانونی به سیستم‌های فناوری اطلاعات نقض تمامیت ارضی کشور است (Schmitt & Vihul, n.d.). در نتیجه، دولت باید یک سیستم تشخیص نفوذ داشته باشد که به طور مستقل یا از طریق همکاری بین المللی توسعه یافته باشد (رمضان، ۲۰۱۹). اما کتاب راهنمای تالین و گروه کارشناسان دولتی امنیت اطلاعات سازمان ملل متحد اقدامات حاکمیتی کاملی برای رسیدگی به برخوردهای ژئوپلیتیک در فضای سایبری نیستند و دولت‌ها باید از آنها به عنوان یک راهنما و نمونه دستورالعمل استفاده کنند. این اقدام برای اطمینان از عدم تکرار حملات سایبری که ثبات ژئوپلیتیکی را مختل می‌کند مورد نیاز است.

1. UNGGE
2 . The Tallinn Manual