

عمق ژئوپلیتیک دیجیتال (جلد ۲)

تألیف

دکتر افشین متقی دستنائی
استاد جغرافیای سیاسی دانشگاه خوارزمی

دکتر علی کرمی

www.ketab.ir



دانشگاه خوارزمی

تهران ۱۴۰۳

سرشناسه	: متقی دستتایی، افشین، ۱۳۶۲-
عنوان و نام پدیدآور	: عمق ژئوپلیتیک دیجیتال/تالیف افشین متقی دستتایی، علی کرمی.
مشخصات نشر	: تهران: دانشگاه خوارزمی، ۱۴۰۳-
مشخصات ظاهری	: ج. ۲.
شابک	: دوره 5-978-622-4815-09-5 ج. ۱. 978-622-4815-10-1 ج. ۲. 978-622-4815-11-8
وضعیت فهرست نویسی	: فیبا
یادداشت	: کتابنامه.
موضوع	: سیاست جغرافیایی Geopolitics فضای مجازی - جنبه های سیاسی Cyberspace -- Political aspects جغرافیای سیاسی Political geography
شناسه افزوده	: کرمی، علی، ۱۳۶۲- دانشگاه خوارزمی
رده بندی کنگره	: ۳۱۹/۱۲
رده بندی دیویی	: ۳۱۹/۱۲
شماره کتابشناسی ملی	: ۹۶۹۷۴۳۴
اطلاعات رکورد کتابشناسی	: فیبا



دانشگاه خوارزمی

عنوان کتاب	: عمق ژئوپلیتیک دیجیتال (جلد ۲)
تألیف	: دکتر افشین متقی دستتایی، دکتر علی کرمی
ناشر	: دانشگاه خوارزمی
چاپ و صحافی	: دانشگاه خوارزمی
صفحه آرا	: مسعود سلیمانی
طراح جلد	: مسعود سلیمانی
نوبت و سال چاپ	: اول، ۱۴۰۳
شابک دوره	: ۹۷۸-۶۲۲-۴۸۱۵-۰۹-۵
شابک جلد دوم	: ۹۷۸-۶۲۲-۴۸۱۵-۱۱-۸
شمار	: ۵۰۰ نسخه
قیمت	: ۵۰۰۰۰۰۰ ریال

کلیه حقوق مادی و معنوی این اثر متعلق به انتشارات دانشگاه خوارزمی است.

آدرس: تهران، خ شهید مفتاح، شماره ۴۳، کدپستی ۱۴۹۱۱-۱۵۷۱۹ تلفن مرکز پخش: ۸۸۳۱۱۸۶۶

pub@khu.ac.ir

www.khu.ac.ir

فهرست مطالب

۳۹	پیشگفتار.....
۴۳	فصل اول: زیرساخت‌های سایبری مقاوم و عمق ژئوپلیتیک دیجیتال.....
۴۳	تعریف زیرساخت سایبری.....
۴۶	لایه‌های زیرساخت سایبری.....
۴۷	اهداف زیرساخت‌های سایبری.....
۴۹	تاریخچه زیرساخت سایبری.....
۵۴	اجزای زیرساخت سایبری.....
۵۴	۱- منابع انسانی.....
۵۴	۲- نرم افزار.....
۵۵	۳- سخت افزار.....
۵۵	۴- ابزارها و منابع.....
۵۶	۵- هماهنگی و همکاری.....
۵۶	۶- پشتیبانی از چندین کاربر به طور همزمان.....
۵۷	نقش زیر ساخت‌های سایبری در قدرت ملی.....
۵۸	۱. قدرت اقتصادی.....
۵۸	۲. قدرت نظامی.....
۵۹	۳. قدرت فناورانه.....
۵۹	۴. قدرت دیپلماتیک.....
۶۰	زیرساخت‌های سایبری و اقتصاد دیجیتال.....
۶۳	زیرساخت‌های سایبری و قدرت دیجیتال.....
۶۴	اهمیت ژئوپلیتیکی زیرساخت‌های سایبری.....
۶۹	زیرساخت‌های سایبری مقاوم.....
۷۳	ژئوپلیتیک زیرساخت‌های سایبری.....
۷۵	ارزیابی امنیت زیرساخت سایبری.....

۷۸	تقابل سیاست‌های توسعه زیرساخت‌های سایبری.....
۸۰	زیرساخت‌های سایبری پایدار و عمق ژئوپلیتیک دیجیتال.....
۸۲	۱- تاب آوری زیرساخت.....
۸۲	۲- اتصال جهانی.....
۸۳	۳- حاکمیت داده.....
۸۴	۴- نوآوری فناوریانه.....
۸۵	۵- همکاری امنیت سایبری.....
۸۶	۶- رقابت ژئوپلیتیکی.....
۸۷	افزایش تهدیدات سایبری در ژئوپلیتیک.....
۹۰	رقابت ژئوپلیتیکی و تأثیر محلی.....
۹۳	فصل دوم: قدرت سایبری و عمق ژئوپلیتیک دیجیتال.....
۹۳	اهمیت ژئوپلیتیکی قدرت سایبری.....
۹۶	اهمیت قدرت سایبری برای عمق ژئوپلیتیک دیجیتال.....
۹۹	قدرت سایبری.....
۹۹	۱- امنیت سایبری.....
۱۰۲	۲- جنگ سایبری.....
۱۰۵	۳- اطلاعات سایبری.....
۱۰۶	۴- زیرساخت سایبری.....
۱۰۸	۵- خط‌مشی‌ها و مقررات سایبری.....
۱۱۰	۶- آموزش و نیروی کار سایبری.....
۱۱۱	۷- دیپلماسی سایبری.....
۱۱۳	۸- تاب آوری سایبری.....
۱۱۴	اکوسیستم ملی قدرت سایبری.....
۱۱۶	ارکان استراتژی ملی سایبری.....
۱۱۷	ویژگی‌های یک قدرت سایبری پیشرو جهانی.....
۱۱۹	زیرساخت‌ها و قدرت دیجیتال.....
۱۲۰	دفاع سایبری ملی.....
۱۲۲	استعمار داده دیجیتال.....

۱۳۰	حاکمیت داده.....
۱۳۲	جایگاه ابر رایانه‌ها در قدرت دیجیتال.....
۱۳۳	۱- شبیه‌سازی‌های پیشرفته.....
۱۳۴	۲- تجزیه و تحلیل داده‌های بزرگ.....
۱۳۵	۳- هوش مصنوعی و یادگیری ماشینی.....
۱۳۶	۴- کشف دارو و مراقبت‌های بهداشتی.....
۱۳۶	۵- امنیت ملی و دفاع.....
۱۳۸	۶- پیش‌بینی آب و هوا و تحقیقات آب و هوا.....
۱۳۸	ماهواره‌ها و قدرت دیجیتال.....
۱۴۲	نیمه هادی‌ها و قدرت دیجیتال.....
۱۴۴	جایگاه نیمه هادی‌ها در عمق ژئوپلیتیک دیجیتال.....
۱۴۵	۱- رهبری فناوری.....
۱۴۷	۲- تاثیر اقتصادی.....
۱۴۹	۳- امنیت زنجیره تامین.....
۱۵۰	۴- فن‌آوری‌های دفاعی و استراتژیک.....
۱۵۲	۵- تجارت و مالکیت فکری.....
۱۵۴	۶- اتحادها و رقابت‌های ژئوپلیتیکی.....
۱۵۷	۷- فناوری‌های نوظهور و استراتژی‌های ملی.....
۱۶۱	فصل سوم: استقلال سایبری و عمق ژئوپلیتیک دیجیتال.....
۱۶۱	استقلال سایبری و عمق ژئوپلیتیک دیجیتال.....
۱۶۳	حاکمیت سایبری.....
۱۶۶	۱- خط‌مشی‌ها و رویه‌ها.....
۱۶۶	۲- مدیریت ریسک.....
۱۶۶	۳- انطباق.....
۱۶۶	۴- آگاهی و آموزش.....
۱۶۶	۵- نظارت و شناسایی.....
۱۶۶	۶- واکنش به حادثه.....
۱۶۷	۷- ساختار حاکمیتی.....

۱۶۷	۸-بهبود مستمر.....
۱۶۹	خطرات سیاسی اینترنت.....
۱۷۲	۱-اطلاعات نادرست و اخبار جعلی.....
۱۷۴	۲-اتاق‌های پژواک و قطبی‌سازی.....
۱۷۵	۳-مداخله خارجی.....
۱۷۷	۴-نگرانی‌های مربوط به حریم خصوصی.....
۱۷۸	۵-آزار و اذیت و ارباب آنلاین.....
۱۸۰	۶-سانسور و مقررات محتوا.....
۱۸۲	دستکاری اطلاعات.....
۱۸۳	رقابت برای کنترل و دسترسی به اینترنت.....
۱۸۸	اینترنت ملی.....
۱۹۰	۱-سانسور و کنترل.....
۱۹۲	۲-نظارت دولتی.....
۱۹۳	۳-حمایت‌گرایی و نگرانی‌های امنیتی.....
۱۹۵	۴-جداسازی و تکه تکه شدن.....
۱۹۶	۵-تهدید آزادی بیان.....
۱۹۸	۶-چالش‌های فنی.....
۱۹۹	۷-پیامدهای بین‌المللی.....
۲۰۱	شبکه ملی اطلاعات.....
۲۰۲	۱-کنترل و ایمن‌سازی.....
۲۰۴	۲-محلی‌سازی داده‌ها.....
۲۰۵	۳-ارتقای خدمات ملی.....
۲۰۶	۴-امنیت سایبری.....
۲۰۸	۵-حاکمیت دیجیتال.....
۲۱۱	فصل چهارم: نوآوری سایبری و عمق ژئوپلیتیک دیجیتال.....
۲۱۱	ژئوپلیتیک نوآوری.....
۲۱۳	اهمیت ژئوپلیتیکی نوآوری سایبری.....
۲۱۵	مسابقه تسلیحاتی سایبری.....

۲۱۷.....	نوآوری سایبری.....
۲۱۸.....	۱-نوآوری نرم افزاری.....
۲۱۹.....	۲-نوآوری سخت افزاری.....
۲۲۰.....	اشکال نوآوری سایبری.....
۲۲۰.....	۱- شناسایی پیشرفته تهدید.....
۲۲۱.....	۲- پروتکل های ارتباطی امن.....
۲۲۳.....	۳- تجزیه و تحلیل رفتاری.....
۲۲۴.....	۴-تهدید انگاری همه کاربران، دستگاه ها و ای پی ها.....
۲۲۵.....	۵-نوآوری های امنیت ابری.....
۲۲۶.....	۶-امنیت اینترنت اشیا.....
۲۲۸.....	۷-اطلاعات تهدید سایبری.....
۲۳۱.....	۸-رمزنگاری ایمن کوانتومی.....
۲۳۲.....	۹-پاسخ خودکار به حمله.....
۲۳۴.....	۱۰-امنیت کاربر محور.....
۲۳۶.....	چرخه دائمی نوآوری.....
۲۳۷.....	حاکمیت سایبری و جریان آزاد اطلاعات.....
۲۳۷.....	۱-چارچوب های سیاسی.....
۲۳۷.....	۲-همکاری بین المللی.....
۲۳۷.....	۳-حریم خصوصی و حفاظت از داده ها.....
۲۳۸.....	۴-استانداردهای امنیت سایبری.....
۲۳۸.....	۵-آزادی اینترنت.....
۲۳۸.....	۶-ظرفیت سازی.....
۲۳۸.....	۷- مشارکت عمومی و خصوصی.....
۲۴۰.....	۸-شفافیت و پاسخگویی.....
۲۴۱.....	ژئوپلیتیک و فناوری.....
۲۴۴.....	فناوری هسته اصلی رقابت ژئواستراتژیک.....
۲۴۶.....	شکاف در ژئوپلیتیک نوآوری.....
۲۵۱.....	نوآوری سایبری و عمق ژئوپلیتیک.....

۲۵۵	فصل پنجم: مشارکت مردم و عمق ژئوپلیتیک دیجیتال
۲۵۵	مشارکت مردم و عمق ژئوپلیتیک دیجیتال
۲۵۶	استراتژی‌های امنیت سایبری مشارکت محور
۲۵۷	۱- همکاری چندجانبه
۲۵۹	۲- مشارکت جامعه
۲۶۲	۳- مشارکت شهروندان
۲۶۴	۴- طراحی کاربر محور
۲۶۵	۵- داده‌های باز و به اشتراک گذاری اطلاعات
۲۶۶	۶- ظرفیت سازی و آموزش
۲۶۷	۷- ایجاد خط مشی مشترک
۲۶۸	۸- ملاحظات اخلاقی
۲۷۲	مشارکت سایبری مردم و قدرت ملی
۲۷۵	نقش مشارکت مردم در حکمرانی
۲۷۸	اهمیت افکار عمومی مجازی
۲۸۰	امکان مشارکت عمومی باز و مبتنی بر واقعیت
۲۸۲	ایجاد اعتماد سیاسی
۲۸۵	سرمایه اجتماعی سایبری
۲۸۷	تاب آوری سایبری
۲۹۲	سیاست گذاری سایبری مشارکت محور
۲۹۳	توانمندی و مشارکت
۲۹۴	ارتقای نقش سواد رسانه ای
۲۹۵	رسانه و روایت سازی
۲۹۸	نبرد روایت ها
۲۹۹	شکل ۱: معمای روایت ها
۳۰۰	نقش رسانه ها در نبرد روایت ها
۳۰۲	شکل دادن به افکار عمومی
۳۰۴	پروپاگاندا
۳۰۶	تنظیم دستور کار

۳۰۹.....	اطلاعات نادرست.....
۳۱۲.....	روایت‌های جایگزین.....
۳۱۵.....	تأثیر بین‌المللی.....
۳۱۷.....	جنگ روانی.....
۳۱۹.....	نقش روایت‌ها در نبرد ژئوپلیتیکی.....
۳۱۹.....	توجیه و مشروعیت‌سازی.....
۳۲۲.....	نمونه‌هایی از نقش رسانه‌ها در روایت‌های ژئوپلیتیک.....
۳۲۳.....	شکل دادن به افکار عمومی.....
۳۲۵.....	ایجاد ائتلاف‌ها و اتحادها.....
۳۲۶.....	مقابله با روایات متخاصم.....
۳۲۸.....	شکل دادن به اولویت‌های سیاسی.....
۳۳۱.....	فضای مجازی و نبرد داستان‌ها و روایت‌ها.....
۳۳۱.....	اطلاعات نادرست و پروپاگاندا.....
۳۳۴.....	فیک نیوزها.....
۳۳۶.....	دیپ فیک.....
۳۳۷.....	تقویت رسانه‌های اجتماعی.....
۳۳۹.....	پیام‌رسانی هدفمند.....
۳۴۱.....	مقابله با روایات.....
۳۴۳.....	عملیات روانی.....
۳۴۴.....	حملات سایبری و جنگ اطلاعاتی.....
۳۴۶.....	روایت‌ها به عنوان سلاح.....
۳۴۸.....	داستان سرایی همه‌جانبه.....
۳۵۱.....	پروپاگاندا و جنگ روانی.....
۳۵۱.....	کمپین‌های دروغ‌پردازی مجازی.....
۳۵۴.....	سناریوهای شبیه‌سازی شده و آموزش.....
۳۵۶.....	عملیات نفوذ تعاملی.....
۳۵۷.....	دیپلماسی دیجیتال و قدرت نرم.....
۳۵۹.....	روایات مشارکتی و تولید مشترک.....

۳۶۱	نگرانی‌های اخلاقی و حریم خصوصی.....
۳۶۲	پساحقیقت.....
۳۶۵	جنگ ترکیبی.....
۳۶۹	جنگ شناختی.....
۳۷۲	ارتش سایبری.....
۳۷۶	چگونگی دفاع مردم از منافع ملی در فضای سایبری.....
۳۷۸	اهمیت ساماندهی مردم در فضای سایبری.....
۳۸۰	بسیج دیجیتال.....
۳۸۷	۱- لیگ دفاع سایبری استونی.....
۳۸۸	۲- واحد ۸۲۰۰ اسرائیل (فلسطین اشغالی).....
۳۹۱	فصل ششم: سواد دیجیتال و عمق ژئوپلیتیک دیجیتال
۳۹۱	تحول دیجیتالی قدرت ژئوپلیتیک.....
۳۹۳	نفوذ اطلاعات.....
۳۹۵	جنگ سایبری و امنیت.....
۳۹۵	پویایی اقتصادی.....
۳۹۶	نظارت و کنترل.....
۳۹۶	نوآوری تکنولوژیک.....
۳۹۶	اتحادها و رقابت‌های ژئوپلیتیکی.....
۴۰۱	چیستی سواد در عصر قدرت دیجیتال.....
۴۰۲	سواد اطلاعاتی.....
۴۰۲	سواد رسانه‌ای.....
۴۰۲	سواد فناورانه.....
۴۰۳	شهروندی دیجیتال.....
۴۰۴	تفکر انتقادی.....
۴۰۴	سازگاری و یادگیری مادام‌العمر.....
۴۰۶	سواد دیجیتال.....
۴۱۱	سواد دیجیتال و عمق ژئوپلیتیک.....
۴۱۱	دسترسی به اطلاعات.....

۴۱۱	تفکر انتقادی و تحلیل
۴۱۱	نهادهای مشارکت و مشارکت مدنی
۴۱۲	حمایت از حقوق دیجیتال
۴۱۲	رقابت و نوآوری جهانی
۴۱۲	شکاف در ژئوپلیتیک دیجیتال
۴۱۵	سواد ژئوپلیتیک دیجیتال
۴۱۵	۱- امنیت سایبری و جنگ سایبری
۴۱۵	۲- حاکمیت داده ها
۴۱۶	۳- حکمرانی بر اینترنت
۴۱۶	۴- تجارت دیجیتال و روابط اقتصادی
۴۱۶	۵- رقابت ژئوپلیتیکی در فناوری های نوظهور
۴۱۷	۶- جنگ اطلاعاتی و عملیات نفوذ
۴۱۷	۷- حقوق دیجیتال و حقوق بشر
۴۱۹	فصل هفتم: سواد رسانه ای و عصر ژئوپلیتیک دیجیتال
۴۱۹	سواد رسانه ای و عصر ژئوپلیتیک دیجیتال
۴۲۲	تحولات مفهوم سواد در عصر دیجیتال
۴۲۲	اصول سواد رسانه ای
۴۳۵	جنگ رسانه ای ژئوپلیتیک
۴۳۵	پروپاگاندا و اطلاعات نادرست
۴۳۶	تاکتیک های جنگ اطلاعاتی
۴۳۶	نبرد برای کنترل روایت
۴۳۷	فرافکنی قدرت نرم
۴۳۸	اسلحه سازی رسانه های اجتماعی
۴۴۰	پروپاگاندا و اطلاعات نادرست
۴۴۱	عملیات نفوذ
۴۴۲	حملات سایبری و جنگ اطلاعاتی
۴۴۳	عملیات روانی
۴۴۵	تبلیغات هدفمند و هدف گذاری خرد

۴۴۷		قطبی شدن و تفرقه افکنی
۴۴۸		چالش‌های نظارتی و نگرانی‌های اخلاقی
۴۴۹		اقدامات متقابل و تاب آوری
۴۵۱		ابزارهای رسانه‌ای رقابت ژئوپلیتیکی
۴۵۱		رسانه‌های دولتی
۴۵۲		شبکه‌های پخش بین‌المللی
۴۵۲		۱- ترویج منافع ملی
۴۵۳		۲- ارائه منابع اطلاعاتی جایگزین
۴۵۴		۳- دیپلماسی فرهنگی
۴۵۵		پلتفرم‌های رسانه‌های اجتماعی
۴۵۶		عملیات سایبری
۴۵۷		کمپین‌های اطلاعاتی
۴۵۸		دیپلماسی فرهنگی
۴۵۸		دیپلماسی عمومی و ارتباطات استراتژیک
۴۵۹		مشارکت رسانه‌ای و عملیات نفوذ
۴۵۹		سواد رسانه‌ای مکمل حکمرانی فضای مجازی
۴۵۹		امکان ناپذیری سواد رسانه‌ای و ضرورت حکمرانی غیر لیبرالی
۴۶۳		فصل هشتم: تولید محتوا و عمق ژئوپلیتیک دیجیتال
۴۶۳		جایگاه تولید محتوا در قدرت دیجیتال ملی
۴۷۱		تکنیک‌های تولید محتوای دیجیتال
۴۷۴		ژئواکونومیک دیجیتال
۴۷۸		موج سوم تکامل تمدن
۴۷۸		۱- فناوری اطلاعات
۴۸۰		۲- جهانی شدن
۴۸۱		۳- اقتصاد دانش
۴۸۳		۴- تغییر در الگوهای کاری
۴۸۵		۵- تغییرات فرهنگی
۴۸۷		قدرت ارتباطی رایانه

۴۸۷.....	رژیم‌های پردازش اطلاعات.....
۴۸۹.....	تولید محتوای دیجیتال.....
۴۹۰.....	تبلیغات رسانه‌ای و دیجیتال.....
۴۹۰.....	۱. مشخص بودن هدف.....
۴۹۱.....	۲. درک مخاطب هدف.....
۴۹۱.....	۳. تحقیق و ایده پردازی.....
۴۹۱.....	۴. ساخت پیام.....
۴۹۱.....	۵. ایجاد محتوا.....
۴۹۲.....	۶. طراحی و قالب.....
۴۹۲.....	۷. استراتژی‌های پلتفرم خاص.....
۴۹۳.....	۸. تست و بهینه سازی.....
۴۹۳.....	۹. انطباق و اخلاق.....
۴۹۳.....	۱۰. استراتژی‌های پس از انجام تبلیغات.....
۴۹۴.....	تاریخچه تبلیغات رسانه‌ای و دیجیتال.....
۴۹۶.....	انواع تبلیغات دیجیتال.....
۴۹۸.....	استفاده از روایت سازی و داستان سرایی در تبلیغات دیجیتال.....
۵۰۰.....	۱. کمپین دریم کریزی نایک.....
۵۰۱.....	۲. کمپین همیشه - مثل یک دختر.....
۵۰۱.....	۳ - کمپین زیبایی واقعی داو.....
۵۰۱.....	۴ - کمپین ما اینجا هستیم ایربی انبی.....
۵۰۲.....	۵. کمپین جستجوی سال گوگل.....
۵۰۲.....	۶. کمپین‌های تبلیغاتی کریسمس جان لوئیس.....
۵۰۲.....	۷. کمپین «به اشتراک گذاری یک کوکا» کوکاکولا.....
۵۰۳.....	اثرات سیاسی تبلیغات دیجیتال.....
۵۰۵.....	اثرات ژئوپلیتیکی تبلیغات دیجیتال.....
۵۰۶.....	تولید محتوای دیجیتال و قدرت نرم.....
۵۰۶.....	۱- دیپلماسی فرهنگی.....
۵۰۷.....	۲- رسانه و صدا و سیما.....

۵۰۸.....	۳-زبان و آموزش.....
۵۰۹.....	۴-نوآوری و فناوری.....
۵۱۰.....	۵-تاثیر رسانه‌های اجتماعی.....
۵۱۲.....	۶- هنر و اخلاقیت دیجیتال.....
۵۱۳.....	۷-نفوذ فرهنگی.....
۵۱۵.....	۸-دسترسی جهانی.....
۵۱۶.....	۹-دیپلماسی و دیپلماسی عمومی.....
۵۱۷.....	۱۰-دیپلماسی نرم.....
۵۱۸.....	۱۱-رقابت قدرت نرم.....
۵۲۰.....	۱۲-طرح قدرت نرم.....
۵۲۱.....	۱۳-مشارکت جوانان.....
۵۲۲.....	ژئوکالچر دیجیتال.....
۵۲۵.....	محتوای دیجیتال فرهنگی.....
۵۲۷.....	انعکاس ارزش‌های ملی در تولید محتوای دیجیتال.....
۵۲۹.....	ارزش‌های دینی در تولید محتوای دیجیتال.....
۵۳۱.....	تولید محتوای دیجیتال ایدئولوژیک.....
۵۳۲.....	تولید محتوای دیجیتال و عمق ژئوپلیتیک.....
۵۳۵.....	۱- عمق تحلیلی.....
۵۳۷.....	۲-عمق چند رسانه‌ای.....
۵۳۸.....	۳-عمق بین رشته‌ای.....
۵۳۹.....	۴-عمق جهانی.....
۵۴۱.....	۵-عمق آینده‌نگاری.....
۵۴۵.....	فصل نهم: حکمرانی فضای مجازی و عمق ژئوپلیتیک دیجیتال
۵۴۵.....	حکمرانی فضای مجازی و عمق ژئوپلیتیک دیجیتال.....
۵۵۳.....	حکمرانی فضای مجازی.....
۵۵۷.....	ژئوپلیتیک حکمرانی فضای مجازی.....
۵۵۸.....	حوزه‌های حکمرانی فضای مجازی.....
۵۶۰.....	سطوح جغرافیایی حکمرانی فضای مجازی.....

۵۶۰	 سطح جهانی
۵۶۱	 سطح منطقه ای
۵۶۱	 سطح ملی
۵۶۲	 سطح محلی
۵۶۳	 مدل های حکمرانی فضای مجازی
۵۶۶	 ۱- مدل حکمرانی لیبرال (چند ذینفعی (آزاد و بدون محدودیت))
۵۶۸	 ۲- حکمرانی دولتی
۵۷۰	 آزاد و بدون محدودیت در مقابل مرزبندی و نظارت
۵۷۲	 سواد رسانه ای و حکمرانی فضای مجازی
۵۷۸	 نقش حکمرانی دیجیتال در قدرت دیجیتال
۵۸۳	 منابع

فهرست اشکال و جداول

۱۲۶.....	تصویر ۱. نقشه اتصال اینترنتی در جهان
۱۳۰.....	تصویر ۲. موقعیت مراکز بزرگ داده در جهان
۱۳۳.....	تصویر ۳. موقعیت جغرافیایی صاحبان ابررایانه‌ها در جهان
۱۴۲.....	تصویر ۴. موقعیت جغرافیایی کشورهای دارای بیشترین تعداد ماهواره‌ها
۱۶۰.....	تصویر ۵. موقعیت جغرافیایی کشورهای تولیدکننده نیمه هادی‌ها
۲۹۹.....	شکل ۱. معمای روایت‌ها
۴۰۸.....	جدول ۱. مدل‌های آموزش سواد دیجیتال در جهان
۴۲۴.....	جدول ۲. مهمترین مراحل تحول مفهوم سواد
۴۲۶.....	جدول ۳. مقایسه ویژگی‌های اصلی دو پارادایم ارتباطات جمعی و ارتباطات چند رسانه‌ای
۴۳۰.....	جدول ۴. مدل‌های مختلف آموزش سواد رسانه‌ای در جهان
۵۵۴.....	جدول ۵. مهم‌ترین موضوعات حکمرانی فضای مجازی
۵۶۴.....	جدول ۶. مدل‌های حکمرانی فضای مجازی

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 آپسلائی 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 شئون زندگی بشر سایه افکند. بطوریکه امروزه حیات بشری به فضای مجازی وابسته شده و این وابستگی در آینده نیز گسترش بیشتری خواهد یافت که اگر سیاستمداران، معماران و طراحان فضای مجازی مراقبت نمایند، در آینده ای نه چندان دور بشریت شاهد گرفتار شدن در دام 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 ظرفیتهای 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 بین‌المللی تبدیل شده است.

از آنجاییکه موضوع جغرافیای سیاسی را مطالعه بعد سیاسی فضای جغرافیایی در مقیاسها و گونه‌های مختلف تشکیل می‌دهد، 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 می‌کند.

با توجه به گسترش خارق‌العاده فضای مجازی و نقش بنیادی آن در همه شئون زندگی انبای 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 یافته‌های خود را برای بهره‌برداری در معرض دید علاقمندان قرار دهند.

همت و پشتکار استادان ارجمند و محترم عزیز: جناب آقای دکتر افشین متقی دستنای 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 می‌باشد، که کمک زیادی به تقویت ادبیات و قلمرو معرفتی جغرافیای سیاسی می‌نماید. بنده به سهم خودم صمیمانه از آنان تشکر و قدردانی می‌نمایم.

امیدوارم حاصل کار و تلاش آن‌ها مورد بهره‌برداری علاقمندان بویژه اساتید و دانشجویان ارجمند رشته جغرافیای سیاسی در دانشگاه‌ها قرار بگیرد.

دکتر محمدرضا حافظ نیا

تهران - مردادماه ۱۴۰۳

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 تصویری 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 دعوای رایج این است که فضای دیجیتال واقعی است اما واقعیت ندارد. استفاده تهاجمی و تدافعی از فضای دیجیتال همان اثبات واقعیت داشتن آن است.

ژئوپلیتیک، علمی میان رشته‌ای است که دائماً در حال تولید مشترک با رشته‌های دیگر است و از این طریق پسوندها و پیشوندهای گوناگون بدان اضافه می‌گردد. این ویژگی نشان از خطری 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 کنونی را نیز در خود جای دهد. فضای دیجیتال یکی از مهم ترین این الزامات است. اینجاست که شاهد باز ترکیب 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 که 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 می شود که در آن رویدادها رخ می دهند و اشیا و افراد وجود دارند. مکان اغلب بر حسب فواصل، مختصات و مرزهای فیزیکی توصیف می شود. فضا به طور کلی خنثی یا خالی از معنای خاص در نظر گرفته می شود تا زمانی که فعالیت ها یا ادراکات انسان به آن اهمیت بدهد. فضای بین دو ساختار یا فضای درون یک اتاق نمونه هایی هستند که ابعاد فیزیکی بدون معنای ذاتی تعریف می شوند. مکان فضایی است که با فعالیت ها و تجربیات افراد در آن معنا یافته است. مکان ها آمیخته به اهمیت فرهنگی، اجتماعی و عاطفی هستند که آن ها را از یکدیگر متمایز می کند. آن ها به شکل گیری

هویت و حافظه برای افراد و جوامع کمک می‌کنند. فضا انتزاعی‌تر و کلی‌تر است، در حالی که مکان مشخص‌تر و خاص‌تر است. فضا تا زمانی که از طریق تجربه و ادراک انسان به مکانی تبدیل شود فاقد معنای ذاتی است. مکان‌ها محل وقوع فعالیت‌های انسانی و شکل‌گیری روابط اجتماعی هستند، در حالی که فضا پس‌زمینه‌ای است که این فعالیت‌ها در آن صورت می‌گیرد. 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 ژئوپلیتیک دیجیتال کدام‌اند. عمق ژئوپلیتیک دیجیتال متشکل از مولفه‌هایی است که سنجش و مقایسه کمی و کیفی آن‌ها تعیین‌کننده سطح عمق ژئوپلیتیک دیجیتال یک واحد سیاسی است. مهم‌ترین این مولفه‌ها عبارت‌اند از: کمیت و کیفیت زیرساخت اینترنت، به‌طور قابل توجهی بر عمق ژئوپلیتیک دیجیتال یک کشور تأثیر می‌گذارد و بر ابعاد اقتصادی، سیاسی، اجتماعی و فناوری آن تأثیر می‌گذارد. اینترنت با کیفیت بالا به کسب و کارها اجازه می‌دهد تا به‌طور کارآمد فعالیت کنند، نوآوری را تقویت کرده و دسترسی به بازارهای جهانی را ممکن می‌سازد. کشورهای دارای زیرساخت اینترنتی قوی می‌توانند از تجارت الکترونیک، فین‌تک و سایر صنایع دیجیتال پشتیبانی کنند. سرمایه‌گذاری خارجی را جذب می‌کنند، زیرا شرکت‌ها مناطقی با زیرساخت دیجیتال قوی را برای راه‌اندازی عملیات ترجیح می‌دهند. اینترنت سریع و قابل اعتماد با برقراری ارتباط کارآمد، کاهش زمان خرابی و تسهیل کار از راه دور، بهره‌وری را افزایش می‌دهد، که می‌تواند منجر به تاب‌آوری نیروی کار و سازگارتر شود. کشورهایی با قابلیت‌های دیجیتال پیشرفته می‌توانند تأثیر بیشتری در صحنه جهانی داشته باشند. می‌توانند در سیاست‌گذاری دیجیتال بین‌المللی شرکت کنند و از منافع خود دفاع کنند. زیرساخت قوی اینترنت برای امنیت ملی بسیار مهم است. حفاظت بهتر در برابر تهدیدات سایبری را امکان‌پذیر می‌کند، که برای حفظ ثبات سیاسی و حفاظت از اطلاعات حیاتی ضروری است. دسترسی به اینترنت با کیفیت 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 دیجیتالی 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 دیجیتالی کمک می‌کند و تضمین می‌کند که همه اقشار جامعه می‌توانند 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 رایانش ابری استفاده کنند. یک زیرساخت اینترنتی قوی از رشد استارت‌آپ‌های فناوری و مراکز نوآوری پشتیبانی می‌کند و به یک شکل‌گیری اکوسیستم فن‌آوری فعال کمک می‌کند. همچنین توسعه شهرهای هوشمند و برنامه‌های کاربردی اینترنت اشیا به اتصال به اینترنت پرسرعت و قابل اعتماد بستگی دارد. زیرا می‌تواند مدیریت شهری را بهبود بخشد و کیفیت زندگی را افزایش دهد. کشورهای دارای اینترنت قوی می‌توانند تولید و توزیع محتوای دیجیتال در سطح جهانی به نیروگاه‌های فرهنگی تبدیل شوند. محتوای دیجیتال شامل سرگرمی، اخبار و محتوای آموزشی باشد که بر فرهنگ و ارزش‌های جهانی تأثیر می‌گذارد. بخش‌های دیجیتال می‌توانند برای نمایش فرهنگ، ارزش‌ها و ایدئولوژی‌های یک کشور و تقویت قدرت نرم آن در صحنه بین‌المللی استفاده شوند. مثلاً کره جنوبی که در سطح جهانی به دلیل کمیت و کیفیت اینترنت شناخته شده است، از این امر برای تبدیل شدن به یک رهبر در فناوری، سرگرمی (به عنوان مثال، کی‌پاپ 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 کشورها نشان می‌دهند که چگونه سرمایه‌گذاری‌های قابل توجه در زیرساخت‌های اینترنتی می‌تواند از نوآوری‌های تکنولوژیکی، رشد اقتصادی و نفوذ جهانی حمایت کند. بنابراین کمیت و کیفیت اینترنت 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 آنها را در اولویت قرار می‌دهند، در واقع خود را به عنوان ریشرو در عصر دیجیتال می‌شناسانند.

مؤلفه 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 امنیتی سایبری قوی از بانک‌ها و مؤسسات مالی در برابر حملات سایبری محافظت می‌کند و ثبات و یکپارچگی سیستم‌های مالی را تضمین می‌کند. کسب و کارها بیشتر در محیط‌هایی فعالیت می‌کنند که احساس می‌کنند دارایی‌های دیجیتالشان امن است. امنیت سایبری موثر باعث افزایش اعتماد و اطمینان سرمایه‌گذاران داخلی و خارجی می‌شود. حملات سایبری می‌تواند منجر به خسارت اقتصادی قابل توجهی به دلیل سرقت مالکیت معنوی، اختلال در عملیات و آسیب به اعتبار برند شود. امنیت سایبری قوی این خطرات را به حداقل می‌رساند. کشورها و ملت‌ها با تهدیدات ناشی از جنگ سایبری و پروتست‌ها، 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 نظامی مدرن به شدت به سیستم‌های دیجیتال برای ارتباطات، اطلاعات و تسلیحات متکی است. 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 و به عنوان شرکای قابل اعتماد در همکاری‌های بین‌المللی و توافق‌نامه‌های دفاعی دیده می‌شوند. نشان دادن تخصص در امنیت سایبری می‌تواند قدرت نرم یک کشور را تقویت کند. با ارائه کمک‌های امنیت سایبری به سایر کشورها، یک کشور می‌تواند حسن نیت دیپلماتیک ایجاد کند و روابط بین‌المللی 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 سرمایه‌گذاری 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 آنها را به حداقل برساند و به بهبود سریع کمک کند. ارتقاء آگاهی و آموزش امنیت سایبری در میان مردم، انعطاف‌پذیری جامعه را در برابر تهدیدات سایبری افزایش می‌دهد. از آنجایی که کشورها دستخوش تحول دیجیتالی می‌شوند، امنیت سایبری تضمین می‌کند که فناوری‌ها و سیستم‌های جدید به طور ایمن و بدون معرفی آسیب‌پذیری‌های جدید به کار گرفته شوند. یک محیط دیجیتال امن، نوآوری را با فراهم کردن فضای امن برای استارت‌آپ‌ها و شرکت‌های فناوری برای توسعه محصولات و خدمات جدید تقویت می‌کند. رژیم صهیونیستی اسرائیل (فلسطین اشغالی) که به صنعت پیشرفته امنیت سایبری خود معروف است، از تخصص خود برای تبدیل شدن به یک رهبر جهانی در فناوری و سایبر* امنیت سایبری استفاده کرده است. یا مثلاً 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، به الگویی برای ایجاد یک جامعه دیجیتال تاب‌آور با اقدامات امنیتی سایبری قوی تبدیل شده است. امنیت سایبری جزء لاینفک عمل ژئوپلیتیک دیجیتال یک کشور است. زیرا پایه ثبات اقتصادی، امنیت ملی و انعطاف‌پذیری اجتماعی است و در عین حال جایگاه و نفوذ بین‌المللی 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 چشم‌انداز دیجیتال جهانی، موقعیت بهتری دارند.

زیرساخت‌های سایبری تاب‌آور 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 تاب‌آور 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. سرمایه‌گذاران بیشتر در کشورهایی با زیرساخت‌های سایبری قوی و تاب‌آور 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 مجدداً بازبایی کند و کشور را در برابر تaktیک‌های 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 بازبایی مؤثر حوادث سایبری را ممکن می‌سازد، اختلالات اجتماعی را به حداقل می‌رساند و بازبایی سریع خدمات را تضمین می‌کند. کشورها دستخوش تحول دیجیتالی می‌شوند، زیرساخت‌های سایبری انعطاف‌پذیر تضمین می‌کند که فناوری‌های جدید به صورت ایمن و بدون ایجاد آسیب‌پذیری به کار گرفته شوند. زیرساخت تاب آور 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 در 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. سرمایه‌گذاری در زیرساخت‌های انعطاف‌پذیر 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 خود شناخته شده است، زیرساخت سایبری انعطاف‌پذیری را توسعه داده است که از موقعیت آن به عنوان یک مرکز مالی و فناوری جهانی پشتیبانی می‌کند. جامعه دیجیتالی استونی برای محافظت از خدمات دولت الکترونیک خود به زیرساخت‌های سایبری انعطاف‌پذیر متکی است و 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 تمرکز می‌کند.

استقلال سایبری، توانایی یک کشور برای حفظ و کنترل زیرساخت‌های فضای سایبری، داده‌ها و قابلیت‌های دیجیتالی خود، یکی از جنبه‌های حیاتی عمق ژئوپلیتیک دیجیتال است. 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 و خطر آسیب‌پذیری و بهره‌برداری را کاهش دهد. یک کشور با کنترل زیرساخت‌های فضای سایبری خود، بهتر می‌تواند از اطلاعات و ارتباطات حساس در برابر فعالیت‌های جاسوسی و جاسوسی خارجی 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 صلاحیت 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 و اجرا کنند و اطمینان حاصل کنند که شیوه‌های مدیریت داده در داخل مرزهای آنها با استانداردهای ملی مطابقت دارد. استقلال سایبری یک کشور را به عنوان یک کشور پیشرو در سیاست و حکمرانی امنیت سایبری جهانی قرار می‌دهد و به آن اجازه می‌دهد بر هنجارها و استانداردهای بین‌المللی 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 آگاه‌تر است. کشور دارای استقلال سایبری مجهزتر برای مدیریت و بازبایی امنیت 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. در پیش گرفته است. روسیه بر استقلال سایبری از طریق تلاش برای ایجاد یک اینترنت مستقل تأکید کرده است که امکان کنترل بیشتر بر زیرساخت‌ها و داده‌های دیجیتال خود 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 نقش مهمی در افزایش عمق ژئوپلیتیک دیجیتال یک کشور ایفا می‌کند. یعنی توسعه و بکارگیری فناوری‌ها و روش‌های جدید در فضای سایبری که به جنبه‌های مختلف قدرت و نفوذ یک ملت کمک می‌کند. نوآوری سایبری کشور را به عنوان یک کشور پیشرو در فناوری قرار می‌دهد 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 کسب و کار را ساده می‌کند، بهره‌وری را افزایش می‌دهد و کارایی عملیاتی را در صنایع مختلف بهبود می‌بخشد.

با توسعه ابزارهای پیشرفته امنیت سایبری، استراتژی‌های دفاع سایبری و قابلیت‌های تهاجمی 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 یک 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. نوآوری سایبری به قدرت نرم یک کشور با نشان دادن مهارت‌های تکنولوژیکی آن و بهر 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 مرتبط با 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. 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 آموزش، ایجاد نیروی کار ماهر است که قادر به پشتیبانی و ارتقای قابلیت‌های سایبری ملی است. 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. 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 و بهترین شیوه‌ها آگاه باشند، بهتر می‌توانند از خود و سازمان‌هایشان در برابر تهدیدات سایبری محافظت کنند. این آگاهی جمعی آسیب‌پذیری‌ها را کاهش می‌دهد و تاب‌آوری 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 موثر از فناوری‌های دیجیتال را دارند. این امر بهداشت کلی سایبری جمعیت را بهبود می‌بخشد و احتمال وقوع حوادث سایبری را کاهش می‌دهد. مشارکت فعال 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 بزرگ 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 امن، 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. 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 و امن‌تر برای همه کمک کنند.

سواد دیجیتال، توانایی جهت‌یابی، 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 می‌گذارد. نیروی کار با سواد دیجیتالی برای رشد اقتصادی و رقابت ضروری است. کارگران با مهارت‌های دیجیتال می‌توانند با فناوری‌های جدید سازگار شوند و بهره‌وری و نوآوری را بهبود بخشند. سواد دیجیتالی فرهنگ نوآوری و کارآفرینی را تقویت می‌کند. افراد با مهارت‌های دیجیتالی می‌توانند استارت‌آپ ایجاد کنند، فناوری‌های جدید توسعه دهند و اشتغال 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 دسترسی دارند، به پر کردن شکاف‌های آموزشی کمک می‌کند. سواد دیجیتالی شامل درک اصول امنیت سایبری، کمک به افراد و سازمان‌ها برای محافظت از خود در برابر تهدیدات سایبری و کاهش آسیب‌پذیری 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 افزایش 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 قادر می‌سازد تا سازماندهی، حمایت و مشارکت در اهداف اجتماعی و سیاسی، تقویت جامعه مدنی و ترویج عدالت اجتماعی. 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 با چالش‌های ضروری مانند مراقبت‌های بهداشتی، بانکی و خدمات اجتماعی به صورت آنلاین دسترسی داشته باشند. 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 ارزش‌های خود را در سطح جهانی از طریق پلتفرم‌های دیجیتال به اشتراک بگذارند و قدرت نرم و نفوذ بین‌المللی خود را افزایش دهند. مهارت در ابزارهای دیجیتال، همکاری بین‌المللی را در تحقیق، نوآوری و سیاست گذاری تسهیل می‌کند و نقش یک کشور را در امور جهانی تقویت می‌کند. 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 رقابت پذیری امکان‌پذیر می‌سازد. به عنوان مثال استونی که به‌خاطر 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 مرتب‌تری 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 آن می‌شود. رویکرد جامع فنلاند به سواد دیجیتال، از جمله ادغام در سیستم آموزشی، منجر به جمعیت بسیار ماهر و نوآور شده است.

سواد رسانه‌ای، 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 تصمیم‌گیری 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. 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 است. 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 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 مادام‌العمر بهبود بخشند. سواد رسانه‌ای مکمل سواد دیجیتال است و مجموعه‌ای از مهارت‌های جامع را برای پیمایش موثر و مسئولانه در دنیای دیجیتال ارائه می‌دهد. آموزش 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 بین‌المللی را تقویت می‌کند.

شهروندان و متخصصان با سواد رسانه‌ای می‌توانند در همکاری‌های رسانه‌ای بین‌المللی 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 و توسط مخاطبان هدف عمل می‌شود، 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، انعطاف پذیری اجتماعی آن را در برابر اطلاعات نادرست و افزایش مشارکت دموکراتیک تقویت کرده است.

تولید محتوای دیجیتال با افزایش ابعاد مختلف نفوذ ملی، 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 بین‌المللی درآمد ایجاد کرد و رقابت اقتصادی را افزایش داد. تولید محتوای دیجیتال، نوآوری در فناوری و توسعه نرم‌افزار را تقویت می‌کند و به اکوسیستم فناوری گسترده‌تر 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. 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 دیجیتالی 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 دسترس‌تر 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 تولید 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 راه‌حل‌های ذخیره سازی داده‌ها می‌شود. تولید محتوای دیجیتال می‌تواند منجر به همکاری‌ها و مشارکت‌های بین‌المللی 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 کی‌پاپ، 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 تیک‌تاک و سرمایه‌گذاری‌های کلان در بازی و فیلم است که حضور فرهنگی جهانی و رشد اقتصادی خود را تقویت می‌کند.

حکمرانی دیجیتال با ایجاد چارچوبی برای مدیریت نظم 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 جمع‌آوری، پردازش و به اشتراک گذاری داده‌ها نظارت می‌کند. این امر اعتماد به خدمات دیجیتال را افزایش می‌دهد و از شیوه‌های داده‌مستول پشتیبانی می‌کند. از 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 است از طریق ابتکاراتی برای بهبود سواد دیجیتال، گسترش دسترسی پهنای باند، و ترویج گنجاندن دیجیتال برای گروه‌های به حاشیه رانده شده. 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 کنترل بر زیرساخت‌ها و فناوری‌های دیجیتال خود را از طریق اقداماتی برای محافظت در برابر مداخله خارجی، ترویج نوآوری داخلی و تاکید بر حاکمیت در فضای سایبری حفظ می‌کند.

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 متنوع‌تر 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. همان‌طور که ابزارهای دیجیتال به طور اجتناب‌ناپذیری 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 بین‌الملل ایجاد می‌کند. بازیگران سنتی در حال بازنگری برای قدرت در این قلمرو ناشناخته به استفاده از استراتژی‌های سنتی ژئوپلیتیک و ژئواکونومیک در فضای 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 کرده 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 تاب‌آوری 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 امنیت از تاب‌آوری 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 امنیتی و تیم‌های واکنش به حادثه. ۶- تاب‌آوری 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: سرمایه‌گذاری 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 شرکای بخش خصوصی برای ارتقای همکاری در زمینه امنیت دیجیتال، اشتراک‌گذاری اطلاعات تهدیدات، ایجاد هنجارهای امنیت دیجیتال و پاسخ به تهدیدات سایبری فرامرزی.

قدرت دیجیتال ملی یا توانایی یک کشور در حوزه دفاع سایبری و تهاجم سایبری، در دنیای مدرن 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 کسب و کارها،

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 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 اختصاصی 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 دیپلماتی 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 محافظت از حقوق حريم خصوصی افراد ضروری است. شهروندان از دولت‌هایشان انتظار دارند که از داده‌های شخصی آنها محافظت کرده و تراکنش‌های آنلاین را ایمن کنند. همچنین سرمایه‌گذاری در تحقیق و توسعه 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 تاب‌آوری 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، سرمایه‌گذاری در دفاع سایبری، حفاظت از زیرساخت‌های حیاتی، توانایی کشور برای جمع‌آوری، تجزیه و تحلیل و به اشتراک گذاری اطلاعات تهدیدات سایبری با شرکای داخلی و بین‌المللی، آموزش امنیت سایبری و توسعه نیروی کار و همکاری بین‌المللی 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 بعضاً 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 رسانه‌ای. 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 فوق‌الذکر چندان برخوردار نیستند و فاقد عمق ژئوپلیتیک هستند اما از لحاظ مولفه‌های عمق ژئوپلیتیک دیجیتال در رتبه‌های بالا قرار دارند. از جمله مولفه‌های عمق ژئوپلیتیک 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 غیره اشاره کرد. با توجه به این مهم در این کتاب قصد داریم مفهوم عمق ژئوپلیتیک دیجیتال را با مفهوم عمق ژئوپلیتیک در معنای کلاسیک تبیین نمائیم.