مجله علمی بین المللی سلام
Salam International Academic Journal
Journal Homepage https://journal.salam.edu.af
سال دهم، شماره ۱۸، خزان ۱۴۰۴هـ ش

امنیت سایبری و استعمار دیجیتال: بررسی وابستگی زیرساخت‌های سایبری کشورهای جنوب به قدرت‌های شمال

پوهنیار عبدالحمید رفعت[1]، نامزد پوهنیار محمد اجمل عزیزی[2]

DOI: 10.64104/v10.Issue18.n4.Fall.2025

تاریخ نشر ۱۴۰۴/۱۱/۳۰ تعداد صفحات ۲۵ از صفحه ۱۱۸ تا ۱۴۳

ISSN 3078-9575 (Print) ISSN 3078-9583 (Online)

چکیده

در عصر تحول دیجیتال، امنیت سایبری به یکی از مؤلفه‌های اساسی امنیت ملی و حاکمیت دولتها تبدیل شده است. کشورهای جنوب جهان با نوعی وابستگی ساختاری به زیرساخت‌های دیجیتال، خدمات ابری، پلتفرم‌های نرم‌افزاری و تجهیزات تخنیکی متعلق به قدرت‌های شمال مواجه اند؛ وابستگی که میتواند زمینه ساز شکل گیری الگوهای نوین «استعمار دیجیتال» گردد.

تحقیق حاضر با رویکرد کیفی و روش توصیفی – تحلیلی، به بررسی ابعاد فنی و سیاسی این وابستگی پرداخته و تلاش نموده است تا با استفاده از چارچوب‌های شناخته شده امنیت سایبری و مدل ارزیابی ریسک (ریسک = تهدید × آسیب پذیری × پیامد)، مفهوم استعمار دیجیتال را از سطح گفتمان سیاسی به سطح تحلیل فنی و قابل سنجش ارتقاء دهد.

یافته‌های تحقیق نشان میدهد که وابستگی در لایه های اطلاعات، شبکه، پلتفرم و زیرساخت فزیکی، میتواند حاکمیت اطلاعاتی، امنیت زیرساخت‌های حیاتی و استقلال فناورانه کشورهای جنوب را تحت تأثیر قرار دهد. همچنین تحلیل‌ها بیانگر آن است که کاهش این وابستگی مستلزم توسعه ظرفیت‌های بومی امنیت سایبری، سرمایه گذاری در نوآوری تخنیکی، ایجاد مراکز عملیات امنیتی ملی، و بازنگری در چارچوب‌های حقوقی بین‌المللی مرتبط با حاکمیت دیجیتال میباشد.

این تحقیق بر اساس مرور نظام مند منابع علمی داوری شده، گزارش‌های رسمی بین‌المللی و تحلیل مطالعات موردی منتخب انجام شده است.

واژگان کلیدی: امنیت سایبری، استعمار دیجیتال، وابستگی سایبری، قدرت‌های شمال، کشورهای جنوب، زیرساخت سایبری.

[1]. عضو کادر علمی دیپارتمنت حقوق، پوهنځی حقوق و علوم سیاسی پوهنتون سلام. Abdulhamidrafat@jmail.com .+93 77 594 1971

[2]. عضو کادر علمی پوهنځی کمپیوتر ساینس، پوهنتون سلام.

طرح تحقیق

الف – بیان مسئله:

با توسعه و گسترش تخنیک های دیجیتال و نقش روز افزون فضای سایبری در تمامی عرصه های زندگی بشر و به خصوصی عرصه های سیاسی، اقتصادی، امنیتی و فرهنگی، وابستگی کشورها به زیرساخت‌های دیجیتال بیش از پیش افزایش یافته است. کشورهای جنوب جهانی، به خصوص در آسیا، آفریقا و آمریکای لاتین، به علت نبود امکانات و توانمندی های تخنیکی ملی، به شدت به خدمات، تجهیزات، نرم افزارها و پلتفرم‌های دیجیتال تولید شده توسط قدرت‌های شمال (مانند ایالات متحده امریکا، اتحادیه اروپا، چین، روسیه وغیره) وابسته اند. این وابستگی سایبری، زمینه ساز نوع جدیدی از استعمار تحت عنوان "استعمار دیجیتال" شده است؛ جریانی که از طریق انحصار اطلاعات و معلومات کاربران چه در سطح دولت و چه در سطح افراد عادی، کنترل زیرساخت‌های سایبری، قوانین و معیار های فنی بین‌المللی و ابزارهای نظارتی، نفوذ و سلطه سیاسی و اقتصادی بر کشورهای جنوب را فوق العاده امکان پذیر ساخته است. چنین شرایطی نه تنها حاکمیت ملی و استقلال سایبری این کشورها را تهدید می کند، بلکه آن ها را در برابر تهدیدات امنیتی سایبری، نشئت اطلاعات، قطع دسترسی به خدمات حیاتی و بحران‌های اجتماعی آسیب پذیر می سازد.

در این بین، سوال اصلی تحقیق این است که وابستگی زیرساخت‌های سایبری کشورهای جنوب به قدرت های شمال چگونه منجر به تضعیف امنیت ملی و شکل گیری استعمار دیجیتال میگردد، و چه راه های حل میتواند این روند را مهار و مدیریت کند؟ ضرورت پرداختن به این مسئله زمانی بیشتر میشود که درک کنیم در جهان امروز، تسلط بر فضای سایبری معادل تسلط بر قدرت جهانی است و غفلت از این حوزه ممکن است کشورها را در برابر سلطه فناورانه و اطلاعاتی بی دفاع سازد. موضوع که فوق العاده خطررات ناشی از آن و هم اضرار بوجود آمده توسط آن هم برای افراد و هم برای دولت ها غیر قابل جبران خواهد بود. بنا امروزه برای دولت های جنوب اشد ضرورت حس میشود که در زمینه استفاده از فضای سایبر و تخنیک که وابسته به آن است و آن را از کشور های شمال وارد میسازد فوق العاده محتاط بوده تا در آینده در دام امپریالیزم استعمار دیجیتالی سقوط ننموده و بتواند این کشور ها در قطار سایر کشور ها به گونه مسالمت آمیز به حیات سیاسی خویش بدون کدام هراس ادامه دهند.

ب – اهداف تحقیق:

در تحقیق هذا میتوان اهداف زیر را به طور مشخص تعیین کرده و راجع به آن ها به جمع آوری مطالب پرداخت:

1. بررسی مفاهیم مرتبط به موضوع و بیان مفاهیم شاخص‌های استعمار دیجیتال در جهان امروز.
2. تحلیل و ارزیابی وابستگی کشورهای جنوب به کشورهای شمال در بخش زیربناهای سایبری.
3. شناخت تهدیدات امنیتی ناشی از وابستگی کشور جنوب به قدرت های شمال در سطح ملی، منطقه ای و بین المللی.
4. بررسی اثرات و پیامد های استعمار دیجیتال بر استقلال سیاسی، اقتصادی، امنیتی، فرهنگی و... کشورهای جنوب.
5. تحلیل نقش کشورهایی مانند امریکا، اتحادیه اروپا، چین و روسیه در سلطه سایبری در قبال کشور های جنوب و بهره برداری های مداخله گرایانه و استعمار گرایانه کشور ها متذکره.
6. بررسی راهکارهای مقابله با استعمار دیجیتال در سطح ملی، منطقه ای و جهانی کشور های جنوب در مقابل سلطه استعمار گرایانه کشور شمال.

7. بیان نمونه های زنده و روشن از اقدامات استعمار گرایانه کشور های شمال در قبال کشور های جنوب.
8. پیشنهاد راه حل ها برای تقویت امنیت سایبری و خود کفایی تکنولوژیکی کشورهای جنوب جهانی در قبال کشور قدرت های شمال.

ج – روش تحقیق:

این تحقیق با رویکرد کیفی و توصیفی- تحلیلی انجام شده است و هدف آن بررسی پیوند میان وابستگی سایبری، استعمار دیجیتال و پیامدهای حقوقی و امنیتی آن برای کشورهای در حال توسعه میباشد.

۱ .طراحی پژوهش: تحقیق حاضر مبتنی بر تحلیل اسنادی *(Document Analysis)* و مرور نظام مند منابع علمی است. در این مطالعه تلاش شده است تا مباحث نظری حوزه حقوق و سیاست با چارچوب‌های فنی امنیت سایبری تلفیق گردد تا تحلیل ها از پشتوانه تخصصی برخوردار باشند.

۲ .منابع و پایگاه‌های اطلاعاتی: برای گردآوری اطلاعات از پایگاه‌های معتبر علمی بین‌المللی از جمله: *Scopus*، *Web of Science*، *Google Schola*، *IEEE Xplore* و *JSTOR* استفاده گردیده است. همچنان گزارش‌های رسمی نهادهای بین‌المللی و اسناد سیاست گذاری امنیت سایبری نیز مورد بررسی قرار گرفته اند.

۳ .کلیدواژه‌ها و بازه زمانی: جستجو با استفاده از کلید واژه‌های فارسی/دری و انگلیسی مانند: استعمار دیجیتال، وابستگی سایبری، حاکمیت دیجیتال، حملات زیرساخت حیاتی، *Cyber Sovereignty*، *Digital Colonialism* و *Critical Infrastructure Cyber Attacks*

انجام شده است است.

۴ .معیارهای ورود و خروج منابع: منابع پذیرفته شده شامل: مقالات علمی داوی شده، کنفرانس‌های معتبر، گزارش‌های رسمی نهادهای بین‌المللی و اسناد سیاستگذاری ملی و بین‌المللی میشود. منابع حذف شده شامل: وبلاگ‌های غیررسمی، مطالب فاقد نویسنده مشخص و منابع بدون استناد معتبر میباشد.

۵ .روش تحلیل داده‌ها: پس از گردآوری منابع، داده‌ها بر اساس تحلیل مضمون *(Thematic Analysis)* دسته بندی گردیدند و در سه محور اصلی تحلیل شدن که شامل: سازوکارهای وابستگی سایبری، ابزارهای اعمال نفوذ و کنترل دیجیتال و پیامدهای حقوقی و امنیتی برای حاکمیت ملی میباشد. برای افزایش دقت تحلیلی، یافته ها با مدل ارزیابی ریسک امنیت سایبری (ریسک = تهدید × آسیب پذیری × پیامد) تطبیق داده شده اند تا نتایج از حالت صرفاً نظری خارج شده و به سطح تحلیلی و سیاستگذاری ارتقاء یابد.

٦ .چارچوب فنی تحلیل امنیت سایبری و حاکمیت دیجیتال: با توجه به ماهیت بین رشته این تحقیق، تحلیل صرفاً سیاسی یا حقوقی نمیتواند پیچیدگی موضوع استعمار دیجیتال را به طور کامل توضیح دهد. بنابراین، در این مطالعه از یک چارچوب فنی امنیت سایبری برای تقویت تحلیل استفاده شده است.

۷ .طبقه بندی تهدیدات سایبری: تهدیدات مورد بررسی در این پژوهش در پنج دسته فنی طبقه بندی میشوند که عبارت اند از: عملیات‌های سایبری دولت محور، حملات زنجیره تأمین*(Supply Chain Attacks)* ، استخراج داده و نظارت گسترده، حملات علیه زیرساخت‌های حیاتی (انرژی، مخابرات، بانکداری) و عملیات‌های نفوذ اطلاعاتی و جنگ شناختی. این طبقه بندی باعث میشود تحلیل‌های سیاسی بر اساس دسته بندی فنی قابل اندازه گیری شوند.

۸ .لایه‌های فنی حاکمیت دیجیتال: برای تحلیل وابستگی سایبری، ساختار دیجیتال کشورها در چهار لایه بررسی میشود:

- **لایه داده *(Data Layer)* :** محل ذخیره سازی، مالکیت و حوزه قضایی اطلاعات.
- **لایه شبکه: *(Network Layer)*** مسیرهای ترافیکی، کنترل*DNS*، کابل‌های زیردریایی.
- **لایه پلتفرم: *(Application Layer)*** وابستگی به شبکه‌های اجتماعی و خدمات ابری خارجی.
- **لایه زیرساخت فیزیکی:*(Infrastructure Layer)*** مراکز داده، تجهیزات مخابراتی، سخت‌افزار.

این تفکیک لایه امکان سنجش دقیق مفهوم «حاکمیت دیجیتال» را فراهم میکند.

۹ .چارچوب‌های بین‌المللی مورد استناد: برای افزایش اعتبار علمی تحلیل، یافته ها با چارچوب‌های شناخته شده جهانی تطبیق داده شده اند، از جمله:

- چارچوب امنیت سایبری *National Institute of Standards and Technology*
- استاندارد مدیریت امنیت اطلاعات *International Organization for Standardization (ISO/IEC 27001)*
- گزارش‌های تهدید سایبری *European Union Agency for Cybersecurity*

استفاده از این چارچوب‌ها موجب میشود پیشنهادهای ارائه شده در پایان مقاله مبتنی بر معیارهای بین‌المللی باشند.

۱۰ .مدل ارزیابی ریسک

برای تبدیل مباحث نظری به تحلیل عملیاتی، از فرمول زیر استفاده شده است: (ریسک = تهدید × آسیب‌پذیری × پیامد). این مدل به سیاست گذاران اجازه میدهد تا میزان خطر وابستگی دیجیتال را به‌صورت اولویت بندی شده ارزیابی نمایند.

د – سوالات تحقیق:

تحقیق حاضر دارای یک سوال اصلی و چندین سوالات فرعی بوده که در ذیل به ترتیب ذکر میگردد.

یک – سوال اصلی تحقیق:

وابستگی کشورهای جنوب به قدرت‌های شمال در بخش زیربناهای سایبری، چگونه باعث پیدایش استعمار دیجیتال و تهدید برای امنیت ملی میشود؟

دو – سوالات فرعی تحقیق:

1. استعمار دیجیتال چیست و از چه زمانی آغاز گردیده است؟
2. قدرت های شمال چگونه از اطلاعات و زیربناهای دیجیتال برای سلطه خویش در قبال کشور های جنوب استفاده میکنند؟
3. سلطه استعمار دیجیتالی کشور های شمال چه پیامدهایی برای استقلال سایبری و ملی کشورهای جنوب دارد؟
4. کدام شرکت های بزرگ فناوری در عرصه استعمار دجیتال فعالیت داشته و نقش این شرکت‌های بزرگ تکنولوژی در این وابستگی چیست؟
5. چه نمونه هایی از جاسوسی سایبری و دخالت در کشورهای جنوب وجود دارد؟
6. برای کاهش وابستگی کشور های جنوب به زیرساخت های سایبری کشور های شمال چه راه های حل قابل تطبیق وجود دارد؟
7. کدام کشور های شمال در عرصه استعمار دجیتال در قبال کشور های جنوب پیشگام میباشند؟

هـ – فرضیه های تحقیق:

در این قسمت به ترتیب از فرضیه اصلی و فرضیه های فرعی تذکر به عمل میآید.

یک – فرضیه اصلی تحقیق:

وابستگی زیرساخت‌های سایبری کشورهای جنوب به فناوری ها و پلتفرم‌های دیجیتال کشورهای شمال، موجب شکل گیری نوعی استعمار نوین به نام استعمار دیجیتال شده است که امنیت ملی، استقلال اطلاعات و توان تصمیم گیری کشورهای جنوب را تهدید میکند.

دو – فرضیه‌های فرعی تحقیق:

1. استعمار دیجیتال مفهومی نوین در روابط بین الملل است که از اوایل قرن ۲۱ با گسترش نفوذ دیجیتالی کشورهای توسعه یافته (کشور های شمال) و شرکت‌های چندملیتی در کشورهای در حال توسعه (کشور های جنوب جهانی) آغاز شده است.
2. قدرت‌های شمال از طریق تسلط بر زیرساخت‌های اینترنتی، ذخیره سازی اطلاعات و پلتفرم‌های ارتباطی، امکان نظارت، تحلیل و هدایت اطلاعاتی کشورهای جنوب را به دست آورده و از آن به عنوان ابزار سلطه استفاده می کنند.
3. سلطه دیجیتالی کشورهای شمال موجب سلب حاکمیت اطلاعاتی، افزایش آسیب پذیری امنیتی و کاهش استقلال سیاسی کشورهای جنوب شده است.
4. شرکت‌های بزرگ فناوری مانند: *Google*، *Amazon*، *Meta*، *Microsoft*، *Apple* وغیره نقش اساسی در کنترل زیرساخت‌ها و اطلاعات کشورهای جنوب دارند و ابزارهای نرم افزاری و خدمات ابری آن ها، زمینه ساز وابستگی سایبری این کشورها شده اند.
5. نمونه هایی از جاسوسی سایبری مانند عملیات *PRISM* توسط آمریکا یا حملات سایبری *Stuxnet* علیه ایران، نشان دهنده نقش برجسته قدرت‌های شمال در مداخلات سایبری علیه کشورهای جنوب است.
6. ایجاد زیرساخت‌های بومی سایبری، سرمایه گذاری در دانش فنی داخلی، همکاری‌های منطقه ای جنوب - جنوب و تدوین قوانین ملی اطلاعات محور، راهکارهای مؤثری برای کاهش وابستگی دیجیتال کشورهای جنوب محسوب میشوند.
7. ایالات متحده آمریکا، اتحادیه اروپا و تا حدودی چین و روسیه، به عنوان کشورهای پیشگام در استعمار دیجیتال شناخته میشوند که از طریق شرکت‌های فناوری و نفوذ سایبری، کشورهای جنوب را در کنترل خود دارند.

و – سازماندهی تحقیق: این تحقیق شامل یک طرح تحقیق (پروپوزال)، هفت مبحث، نتیجه گیری و منابع در اخیر میباشد. مباحث این تحقیق قرار ذیل میباشد: مبحث اول – مفهوم شناسی، مبحث دوم – سیر تاریخی فضای سایبر و امنیت سایبری، مبحث سوم – استعمار دیجیتال، مبحث چهارم – آسیب پزیری و وابستگی کشور های جنوب، مبحث پنجم – قدرت های شمال و سلطه سایبری، مبحث ششم – پیامد های وابستگی سایبری و مبحث هفتم – راهبرد های مقابله با استعمار دیجیتال میباشد.

امنیت سایبری و استعمار دیجیتال

در عصر دیجیتال امروز، فناوری اطلاعات و ارتباطات به ستون فقرات جوامع مدرن تبدیل شده و امنیت سایبری به یکی از مهم ترین ابعاد امنیت ملی کشورها مبدل گشته است. در این میان، کشور های جنوب جهانی که اکثرا شامل کشورهای در حال توسعه اند، به شدت به زیرساخت های فناورانه و سایبری قدرت‌های شمال وابسته اند. این وابستگی، در بسیاری از موارد، به شکل نوعی استعمار نوین یا «استعمار دیجیتال» ظهور یافته است؛ استعمار دیجیتالی که نه با نیروی نظامی، بلکه با ابزارهای فناورانه و اطلاعاتی، سلطه خود را تحمیل میکند. تسلط شرکت‌های بزرگ فناوری، کنترل داده‌ها، و تحمیل الگوهای فرهنگی و امنیتی، از نشانه های بارز این استعمار نو است. این تحقیق میکوشد تا با بررسی ابعاد مختلف وابستگی سایبری کشورهای جنوب، تهدیدهای ناشی از آن را تبیین نموده و راهکارهایی برای کاهش این آسیب پذیری ارائه دهد.

مبحث اول: مفهوم شناسی

در این مبحث به شناسائی و معرفی مفاهیم مرتبط به موضوع تحقیق حاضر ذیلا میپردازیم:

1 – تعریف فضای سایبر: فضای سایبر، یک محیط الکترونیکی و غیر فزیکی است که از طریق آن اطلاعات ایجاد، ارسال، دریافت، ذخیره، پردازش و حذف میگردد (کامران دستجردی حسن و میر محمدی زهرا، 1392، فضای سایبری و تعاریف در جغرافیای سیاسی). فضای سایبر یک فضای غیر مرئی و غیر فزیکی میباشد بر عکس فضای طبیعی که ما در آن جسما سیر کرده میتوانیم اما در فضای سایبر ما جسما سیر و گردش کرده نمیتوانیم بلکه توسط موس کمپیوتر سیر کرده میتوانیم.

2 – امنیت سایبری: امنییت یعنی کاهش خطر و کم ساختن خطر میباشد، امنیت سایبری یعنی محافظت از سیستم ها، شبکه ها، برنامه ها و سامانه های نرم افزاری در برابر حملات دیجیتالی. هدف از امنیت سایبری، محافظت از اطلاعات در برابر سرقت و آسیب است. بدون وجود امنیت سایبری، سازمان ها نمی توانند از خود در برابر نقض های داده ای(*Data Leakese*) و حمله های هکر ها دفاع کنند و به هدفی ساده برای مجرمان سایبری تبدیل میشوند. مخاطرات امنیتی به دلیل گسترده تر شدن ارتباطات در مقیاس جهانی و استفاده از خدمات ابری برای ذخیره سازی اطلاعات حساس و شخصی رو به رو است (انوشا سهیل و همکاران، 1400، سومین همایش ملی تحقیقات میان رسته ای در علوم مهندسی و مدیریت).

3 – جرایم سایبری: جرایم سایبری مجموعه اقداماتی که با انگیزه های مجرمانه و به صورت عمدی علیه شهرت یک فرد یا گروه و یا به منظور آسیب فزیکی و روانی، از طریق شبکه های ارتباطی مدرن مثل اینترنت به صورت مستقیم یا غیر مستقیم انجام میشود (مخمل باف سیده زهره و آزاد شیرزاد، 2020م، مقایسه سیاست های امنیت سایبری رؤسای جمهور آمریکا«2000-2020»). در کل هر اقدام خلاف قانون و نظم عامه که توسط انترنت صورت بگیرد جرایم سایبری است.

4 – جنگ سایبری: جنگ سایبر به هرگونه عمل خصمانه علیه سیستم های کمپیوتری، شبکه های کمپیوتری یا پایگاه های اطلاعات کمپیوتری دشمن اطلاق میشود که با هدف کاهش کارایی یا نا توان سازی صورت پذیرد. حملات سایبری، سیستم های هدف خود را غیر قابل دسترس نموده، کارایی آن ها را کم کرده با تزریق اطلاعات غلط تصمیم گیری کاربران را کاهش می دهند و حتی منجر به سرقت اطلاعات میشوند. به بیان دیگر جنگ سایبر عبارت است از به کار گیری برنامه ریزی شده عملیات آفندی و پدافندی که در آن توسط یک ابزار کمپیوتری علیه ابزار کمپیوتری دیگر حملاتی صورت میگیرد ضمن این که به کارگیری تعمدی ابزار ها و شبکه های کمپیوتری این به منظور اثر گذاری بر تصمیم گیری مخاطبان را نیز باید در زمره

جنگ سایبر به حساب آورد (یادگاری وحید و همکاران، 1396، نقش امنیت فاوا در جنگ سایبری علیه سازمان های امنیتی با رویکرد پدافند غیر عامل).

در مجموع جنگ در فضای سایبر توسط بازیگرانی عمدتا دولتی صورت میگیرد که به دنبال استفاده از این فضا برای رسیدن به اهداف سیاسی، اقتصادی، فرهنگی وغیره خود میباشند.

5 – مفهوم کشور های جنوب و شمال: در میان تقسیم بندی هایی که بر دوگانگی جهان معاصر تأکید میکنند، می توان به تقسیم جهان به دو بخش «شمال» و «جنوب» اشاره کرد. اصطلاح کشور های شمال و جنوب اولین بار توسط یک جغرافیه دان به نام هاوس هوفر در فاصله دو جنگ جهانی اول و دوم به کار برده شد. به اعتقاد وی کشور های قدرتمند و پیشرفته در قسمت شمالی و کشور های جهان سوم در بخش جنوبی کره زمین قرار دارند. درواقع، شمال نشان دهنده کشور های صنعتی قدیم بوده و تنها به جوامع غربی اشاره ندارد و در مقابل جنوب به معنی کشور هایی است که رشد اقتصادی آنها عمدتا به دلیل دوران استعمار به عقب افتاده است. به عقیده هوفر چهار کشور قدرتمند از غرب به شرق عبارت اند از: ایالات متحده امریکا، آلمان، روسیه و جاپان (کلانتری صمد و خلیلی عبدالرسول، 1389، جهانی شدن و روابط شمال و جنوب).

اصطلاح شمال و جنوب بعد از جنگ جهانی دوم، نه در معنی جغرافیه سیاسی فوق، بلکه عمدتا در معنی اقتصادی آن، از سوی محافل سیاسی و دیپلوماتیک و برخی سازمان های بین المللی به کار گرفته شد. این اصطلاح معمولا به جای اصطلاح جهان سوم به کار میرود و البته به موازات این رواج، همان معانی و مفاهیم وسیع و منتوع اقتصادی، سیاسی و اجتماعی را که بر اصطلاح جهان سوم دلات می کرد به خود می گیرد. وقتی این اصطلاح در کشور های موسوم به جهان سوم به کار میرود، به این معنی است که جهان از دو بخش تشکیل شده است: یک بخش شامل کشور های پیشرفته صنعتی، غنی، قدرتمند، به نام شمال و بخش دیگر شامل کشور های کم توسعه، غیر صنعتی، غالبا فقیر و ضعیف، به نام جنوب که در واقع تضاد و رویا رویی در جهان امروزی بین این دو وجود دارد (کلانتری صمد و خلیلی عبدالرسول، 1389، جهانی شدن و روابط شمال و جنوب).

تقسیم جهان به شمال و جنوب از نظر تاریخی حایز اهمیت است اما این تقسیمات در پهلوی بیان حقایق موجود در بین کشور ها، مشکلات و سوء تفاهمات را هم برای انسان ها بوجود آورد. روابط شمال و جنوب به عمده ترین، بغرنج ترین و حساس ترین مسئله قرن بیستم تبدیل شده بود. تقسیم جهان به شمال غنی و جنوب فقیر برای دو نسل، یادآور دو دنیای جدای از هم، نا برابر و متعارض شمرده می شد (ساعی احمد، 1392، جهانی شدن و جنوب). کشور ها در گذشته به جهان اول، دوم و سوم تقسیم میگردیدند اما امروزه این تقسیم بندی جای خود را تا اندازه ای به تقسیم بندی دیگری داده که آن عبارت است از کشور های شمال و کشور های جنوب.

6 – مفهوم زیر ساخت های سایبری: زیرساخت های سایبری، به اجتماع مردم، پردازش ها، سیستم هایی که فضایی سایبر را تشکیل می دهند گفته میشود. زیرساخت های سایبری هشت جزء مهم دارد که ذیلا به آن اشاره مینمائیم:

الف – محیط: ساختمان، محل برج های سلولی، فضایی که ماهواره ها در آن قرار دارند، زمین و دریا که از آن ها کابل عبور کرده وغیره.

ب – انرژی: انرژی شامل برق، باتری، جنراتور ها، پنل های خورشیدی وغیره موارد میشود.

ج – سخت افزار: سخت افزار شامل تراشه های سیمی کانداکتور، کارت های الکترونیکی، سسرور های مداربسته، امکانات فلزی، فیبر نوری وغیره موارد میشود.

د – نرم افزار: نرم افزار در برگیرنده برنامه های چون: کد منبع، برنامه های کامپیوتری، نسخه های کنترل، مدیریت دیجتال، پایگاه اطلاعات وغیره بخش ها میشود.

ه – شبکه: شبکه شامل مسایل از قبیل: نود، ارتباطات، توپولوژی، پروتوکول وغیره میشود.

و – انتقال: انتقال به خدمات از قبیل: انتقال دهنده های اطلاعات بر روی زیر ساخت ها، الگو ها و ارقام ترافیکی، رهگیری اطلاعات وغیره لوازم مورد ضرورت اطلاق میگردد.

ز – انسان: انسان به کار کنان مختلف بخش این زیر ساخت ها گفته میشود که خدمات چون: طراحی، عملی سازی، اپراتوری، تعمیر کاری، نگهداری وغیره امور را عهده دار میباشد.

ح – سیاست: سیاست در اینجا پالیسی های موجود از طروق قانونگذاری را میگوید که شامل: قوانین، طرزالعمل ها، قرارداد ها، توافقات، استاندارد ها، معاهدات و غیره میباشد (کامران دستجردی حسن و میر محمدی زهرا، 1393، فضای سایبر و تعاریف جدید در جغرافیای سیاسی).

این زیر ساخت ها همیشه در حال گسترش میباشد و ممکن است بغیر از موارد فوق الذکر موارد دیگری را هم در بر گیر از قبیل استفاده از ربات ها در بخش های زیربنائی سایبری وغیره.

مبحث دوم – سیر تاریخی فضای سایبر و امنیت سایبری:

در این مبحث، چهار موضوع برای بحث داریم که ذیلا به تک تک آن به گونه جدا جدا خواهیم پرداخت:

1 – تاریخچه فضای سایبر: فضای سایبر به دلیل ظرفیت ها و پتانسیل هایی که دارد محیط بسیار امن و کم هزینه ای را برای ارتکاب حملات سایبری برای دولت ها فراهم آورده است. ترکیب فناوری ارتباطات راه دور با فناوری کامپیوتر در اواخر دهه 1970م و اوایل دهه 1980م «بنیان انقلاب اطلاعاتی حاضر» به عنوان نقطه شروع بحث تهدیدات سایبری به حساب میآید (فرشا سعید پرویز و همکاران، 1401، ضرورت همکاری دولت ها در تقویت امنیت سایبری).

وقتی محصلان پوهنتون استانفورد، بیل هیلیت و دیوپیکا کمپیوتری را به وزن 18 کیلوگرام در سال 1968م ساختند؛ پیش بینی نکرده بودند که تقریبا یک سال بعد کمپیوتر آن ها یک پیام را از کمپیوتر دیگر که در فاصله 569 کیلومتری از آنها در پوهنتون کالیفورنیای لاس آنجلیس قرار دارد، دریافت میکند. آن ها به طور حتم پیشبینی نمیتوانستند که حدود 50 سال بعد، همه چیز از صنعت تا صحت، وابسته به ارتباطات ایجاد شده توسط کمپیوتر ها (انترنت) شود، امروزه، کمپیوتر و انترنت به بخش جدایی ناپذیر زندگی بشر تبدیل شده است (حسینی سید محمد و هاشمی غازی، 1398، حقوق جزای اختصاصی 3). بعد از این که کمپیوتر اختراع گردید و به تعقیب آن ظهور انترنت، زمینه پیدایش فضای سایبر و معضلات مربوط به آن را به وجود آورد.

2 – تاریخچه امنیت سایبری: در کنار چندین ویروس مخرب و انواع بد افزار ها در سناریوی امروز، فکر اینکه فقط چند دهه پیش، هنگام به وجود آمدن شبکه ها و شبکه های جهانی گسترده، امنیت همیشه مهمترین نگرانی نبوده غیر منطقی به نظر میرسد. حتی، در مراحل اولیه به آژانس پروژه های تحقیقاتی پیشرفته و شبکه های مبتنی بر پکت سوئیچ که توسط پنتاگون حمایت مالی میشود، حملات زیادی توسط دانش آموزان دبیرستان انجام شد. به همین ترتیب، میتوان به سناریو های مربوط به (*Talk Talk*) نگاه کرد، که در اوایل، امنیت نداشتند. در یک حمله طولانی، اولین محققان کمپیوتری در جهان به اجرای روش های امنیتی پرداختند. روند هک کردن خطوط تلفن برای ایجاد تماس های رایگان، تکنیکی معروف بود که در دهه 70 و

روز های آغازین کار شبکه ها به کار گرفته شد. یکی از مشهور ترین فریدور ها، جان درایپر، که قبلا فعالیت میکرد و سپس به دلیل حملات مکرر مجازات و دستگیر شد. در سال 1998م رابرت موریس اولین کرم کمپیوتری را در انترنت راه اندازی کرد، که توانست بسیاری از موارد آنلاین را در آن زمان از بین ببرد. اما در اواخر دهه 80م انترنت به عنوان قسمت حیاتی زندگی روزمره ما نبود و عواقب آن به اندازه امروز کار آمد نبود. ویروس یا کرم اولین جرمی شد که تحت قانون تقلب و سوء استفاده کمپیوتری در سال 1986م محکوم شد. این کرم پس از اینکه چندین ویروس اولیه در اوایل دهه 1980م در معرض خطر قرار گرفت، مانند ویروس «مغز» در سال 1986م مورد تبلیغ قرار گرفت (کتانچی الناز و پور قهرمانی بابک، 1399، چالش های امنیت سایبری در کشور های آسه آن). بحث امنیت سایبری در ایالات متحده آمریکا در هه 1970م آغاز گردید در دهه 1980 شتاب گرفت و در اواخر دهه 1990 به سایر کشور ها گسترش یافت. حملات سایبری با اهداف سیاسی یا اقتصادی انجام میگیرند چنانکه در سال 2007م دولت روسیه حملات را علیه کشور استونی انجام داد و همچنین حملات استاکس نت علیه تأسیسات هسته ای ایران در سال 2010م با اهداف سیاسی انجام گرفت. پس از شیوع بیماری کرونا حملات سایبری علیه کشور های مانند بریتانیا، آمریکا و کانادا که جهت تولید واکسن این بیماری در حال تحقیق بودند افزایش یافت. هدف از انجام این حملات سرقت نتیجه تحقیقات در مورد واکسن این بیماری بود. چنین حملاتی بیشتر برای اهداف اقتصادی انجام می گرفت. تاریخ تحولات روابط بین الملل نشان داده است که مقتضیات زمان، به پیچیدگی های مفهوم امنیت افزوده است به ویژه اینکه امروزه کشور ها نمی توانند در معادلات امنیتی و راهبردی خود، از نقش فناوری سایبری و تأثیر آن بر امنیت غافل شوند (فرشا سعید پرویز و همکاران، 1401، ضرورت همکاری دولت ها در تقویت امنیت سایبری).

3 – خصوصیات و ویژگی های فضای سایبر: افزایش میزان وقوع فعالیت های مجرمانه و ظهور احتمالی انواع جدید فعالیت های مجرمانه، چالش هایی را برای نظامهای حقوقی و همچنین برای اجرای قانون ایجاد میکند. در ذیل برخی از اصلی ترین ویژگی های جرایم سایبری آورده میشود:

الف – فناوری دیجیتال: جرایم سایبری به ناچار نوعی فناوری دیجیتال را شامل می شود، از تلفن هوشمند یا کمپیوتر روی میزی گرفته تا اطلاعات رمز گذاری شده یا شبکه های امن.

ب – دانش تخصصی: جرایم سایبری تنها از طریق فناوری قابل ارتکاب است، بنابر این برای ارتکاب این نوع جرایم باید در کمپیوتر و اینترنت مهارت داشته باشد.

ج – آثار شدید: جرایم سایبری به طور فزاینده ای فراگیر و پیچیده می شوند و اثرات اقتصادی شدیدتری نسبت به بسیاری از جرایم متعارف اند.

د – ساختار ویژه: جرایم سایبری از نظر ساختاری از سه طریق اصلی منحصر به فرد هستند آنها از نظر فناوری و مهارت فشرده هستند.

هـ – فقدان اطلاع رسانی: جرایم سایبری نیز از جمله گزارش نشده ترین اشکال جرم و جنایت هستند. بسیاری از قربانیان تمایلی به گزارش جنایات سایبری ندارند زیرا فکر میکنند مراجعه به مجریان قانون مانع حمله نمی شود.

و – نبود علائم و نشانه های ظاهری: برخلاف جرایم سنتی، جرایم سایبری صحنه معمول جرم را در برنمیگیرد و ممکن است تا مدت ها جنایت کشف نشود.

ز – تأثیرات منفی گسترده: یک جرم سایبری در یک زمان محدود می تواند آسیب ها و مشکلات طولانی مدت و گسترده ای را به جامعه و کشور تحمیل نماید (صادقی تاج محمد و همکاران، 1402، کارکرد سازمان های منطقه ای در جنگ های سایبری).

ح – فرامرزی بودن جرم: ماهیت جرایم سایبری فرامرزی است. چون، اینترنت که مجموعه از شبکه های کمپیوتری مرتبط با هم در سطح جهان است؛ در کشور های مختلف کاربرد دارد. اشخاص از سراسر جهان می توانند در فضای سایبر حضور پیدا کنند. این امر هم زمینه ارتکاب جرم فرامرزی و هم زمینه قربانی فرامرزی را ایجاد می کند.

ط – بدون خشونت بودن: جرایم سایبری معمولا جرایم بدون خشونت دانسته می شوند. بر عکس جرایم کلاسیک مثل قتل، تجاوز، اختطاف وغیره. جرایم سایبری بدون درگیری و خشونت ارتکاب می یابد (حسینی سید محمد و هاشمی غازی، 1398، حقوق جزای اختصاصی 3).

ی – دسترسی آسان: عدم تمرکز و دسترسی آسان در هر زمان و مکانی، از جمله ویژگی های ذاتی فضای سایبر است.

ک – تعاملی بودن: در فضای واقعی رفتار ها اغلب جنبه فردی دارد و یک طرفه است مانند راه رفتن، خوردن، نوشتن وغیره، درحالیکه، در فضای سایبر، اساس رفتار یک جانبه بی معنا است و هر کنش و تراکنشی در این فضا، به معنی دادن یا گرفتن اطلاعات " به " یا " از " افراد معلوم یا ناشناس است.

ل – غیر قابل کنترل بودن: غیر ملموس و بی نهایت بودن فضای سایبر، که امکان حضور فزیکی نیروهای بازدارنده را از بین برده است، موجب شده، این فضا، در مصایسه با فضای واقعی، قابلیت کنترل نداشته باشد و هر کاربر حاضر در این فضا، خود را سلطان بلامنازع آن میشمارد.

م – وسعت ضرر و عدم امکان مهار واقعی خسارت: چون زمان و مکان، در فضای سایبر بی معنی است و در خلأ شکل گرفته است، زیان حادثات در این فضا، از لحاظ ماهیت دارای فزایندگی لحظه ای است و به صورت مستمر، با کپی در سایر تارنماها و تخلیه و بارگذاری مجدد در حال تکثیر است (ملکوتی رسول، خلیل زاده مونا، 1400، رهکار حقوقی تأمین امنیت سایبری).

از اینکه فضای حقیقی با فضای مجازی تفاوت دارد، خصوصیات این فضا ها نیز باهم متفاوت میباشد که از جمله خصوصیات فضای سایبر را در فوق تذکر دادیم.

4 – شکل گیری تهدیدات سایبری: ظهور فضای سایبر و شکل گیری ارتباطات از طریق انترنت و اکنون هم هوش مصنوعی تهدیدات سایبری را در تمام عرصه ها و به خصوص عرصه امنیت فوق العاده افزایش داده است. اکثر از تحلیل گران حوزه امنیت، بر این باور اند که پایان یافتن دوران جنگ سرد نه تنها منجر به امن تر شدن جهان نشده است، بلکه به وجود آمدن چالش های امنیتی غیر نظامی جدیدی همچون تخریب محیط زیست، رفاه اقتصادی، سازمان های جنایی بین المللی و مهاجرت گسترده افراد، امنیت جهانی را با چالش های جدی تری نسبت به گذشته مواجه ساخته است. آنچه در مورد این تهدید های جدی قابل توجه است، این است که ویروس ها، کرم ها، جرم ها، هکر ها و حملات انترنتی، امروزه واقعیت مسلم و روزه هستند. حملات مخرب مهم با تأثیرات گسترده، تهدید های سایبری را به عنوان یکی از بدترین تهدید های منافع ملی به تصویر کشیده است تا جایی که امریکا اعلام کرده است که این حملات را به عنوان جنگ تلقی کرده و با آن برخورد فزیکی خواهد کرد (خلیلی پور رکن آبادی علی و نورعلی وند یاسر، 1390، تهدیدات سایبری و تأثیر آن بر امنیت ملی). تهدیدات

امنیتی سنتی اکثرا متوجه ساختار نظامی، دفاعی و امنتی کشور ها میگردد در مقابل قلمرو تهدیدات سایبری همه ابعاد زندگی اجتماعی را در بر میگیرد به خصوص مردم عامه را، در ذیل به بعضی مصادیق تهدیدات سایبری معلومات مختصر ارائه میدارم:

الف – تهدیدات شبکه ای: کاربران، تجهیزات و کانال های ارتباطی (شبکه های بی سیم و سیمی) در معرض انواع مختلفی از تهدیدات سایبری نظیر نفوذ، حمله انکار سرویس، حمله انکار سرویس توزیع شده، حمله سیلابی، بات نت ها، ویروس ها، باج افزار ها وغیره قرار دارند.

ب – تهیدات مرتبط با برنامه ای کاربردی: تمامی برنامه های کاربردی از سامانه های مدیریت بانک های اطلاعاتی گرفته تا برنامه های دسکتاپ، موبایل و سرور ممکن است به آسیب پذیری های آلوده باشند که به هکر ها اجازه دهند به واسطه آن ها به سامانه ها حمله کنند.

ج – تهدیدات دسترسی از راه دور: دسترسی از راه دور یکی از ارکان جتناب ناپذیر کسب و کار های امروزی است. همین مسئله شکاف امنیتی بزرگی به وجود می آورد که در نهایت نقض داده ای را باعث میشود. در این تهدید هکر ها میتوانند رمز عبور و نام حساب کاربری یک کارمند را سرقت نموده و به شکلی کاملا مشروع به شبکه سازمانی نفوذ کنند.

د – تهدیدات دستکاری داده ها: گاهی اوقات حمله های هکری با هدف دستکاری معلومات پایگاه های اطلاعاتی انجام میشوند. در این نوع تهیدات هکر ها پس از نفوذ به یک پایگاه اطلاعات، سعی میکنند با ارتقای سطح دسترسی خود به ویرایش اطلاعات درون پیگاه های اطلاعات و نسخه های پشتیبان آن بپردازند (انوشا سهیل و همکاران، 1400، استراتیژِی امنیت سایبری).

با گذر زمان و گسترش فعالیت های انترنت و هوش مصنوعی تهدیدات سایبری هم گسترش نموده، و این تهدیدات تمام عرصه های زندگی بشر را در بر گرفته و متضرر خواهد نمود.

مبحث سوم – استعمار دیجیتال:

1 – تعریف استعمار دیجیتال: استعمار در لغت به معنی طلب آبادانی است و در اصطلاح، تسلط سیاسی، فرهنگی، و اقتصادی ملتی نیرومند بر ملتی ضعیف و نگه داشتن آنان در وضعیت عقب مانده میباشد؛ استعمار گران به بهانه آباد کردن، وارد یک کشور شده و منابع آن را غارت می کنند؛ بنا به عمل آنان استعمار گفته میشوند (اسکندری مصطفی، 1389، شناخت استعمار).

استعمار دیجیتال به نوعی از سلطه گری نوین گفته می شود که در آن، قدرت‌های بزرگ جهانی از طریق فناوری‌های اطلاعاتی، ابزارهای دیجیتال، داده‌ها و فضای مجازی بر کشورهای ضعیف تر و وابسته تر تسلط می یابند. در این نوع استعمار، به جای اشغال فیزیکی سرزمین‌ها، کنترل بر زیرساخت‌های سایبری، اطلاعات شخصی و ملی، رسانه‌ها، نرم افزارها، و پلتفرم‌های دیجیتال در دستور کار قرار می گیرد. در استعمار دیجیتال، شرکت‌های فناوری محور (مانند گوگل، اپل، مایکروسافت، آمازون و متا) به ابزارهایی برای نفوذ و تسلط قدرت‌های شمال بر کشورهای جنوب تبدیل شده اند. این شرکت‌ها با در اختیار گرفتن داده‌های عظیم و بزرگ (*Big Data*)، الگوهای رفتاری، اقتصادی، فرهنگی و حتی سیاسی جوامع را تحلیل و در مواردی نیز کنترل میکنند (*Coleman Danielle*، 2019، *Digital Colonialism: The 21st Century Scramble for*

Africa through the Extraction and Control of User Data and the Limitations of Data Protection Laws).

استعمار دیجیتال چالش های بزرگی را امروزه در عرصه های مختلف زندگی کشور های جنوب وارد نموده است.

2 – اشکال مختلف استعمار دیجیتالی: استعمار دیجیتال اشکال مختلفی دارد که هر کدام به گونه ای خاص قدرت‌های فناوری را بر کشورهای در حال توسعه و کشور های جنوب مسلط می سازد که در ذیل به بعضی از نمونه های آن اشاره مینمائیم:

الف – تأثیر استعمار دیجیتال در بخش اقتصاد: امروزه یکی از عرصه های که زیاتر مورد حملات سایبری قرار میگیرد و آن را متأثر میسازد بخش اقتصاد است. این بخش از یک سو ستون فقرات جامعه بشری را تشکیل داده و باعث چرخیش زندگی روزمره مردم جهان میشود و از سوی دیگر سایر بخش های زندگی نیز به صورت غیر مستقیم یا هم مستقیم به اقتصاد وابسته میباشد.

حملات سایبری به بخش انرژی، افزون بر هدف به دست آوردن منافع اقتصادی، با هدف وارد کردن خسارت ها و تضعیف اقتصادی دولت های رقیب نیز انجام میشوند. چالش های اقتصادی، بیشترین تهدید های امنیتی وجودی را در بعد سیاسی امنیت ملی به بار میآورد. بیگمان ناتوانی دولت در تأمین نیاز ها و رفاه اقتصادی مردم موجب نارضایتی ملت و به تبع آن کاهش مشروعیت و مقبولیت آن میشود. کاهش توان اقتصادی دولت ها در سطح داخلی زندگی مردم، چنین کشور هایی را تحت تأثیر قرار میدهد و باعث نارضایتی مردم از حکومت ها میگردد. اگر دولت های بتوانند بخش انرژی رقبای خود را از کار بیندارند یا در کار کرد آن ها اختلال ایجاد کنند، میتوانند نارضایتی های گسترده ای را در کشور هایی که هدف این حملات قرار میگیرند، ایجاد نمایند، برای مثال، اگر حملات سایبری بتواند برای مدتی در سامانه های پالایشگاهی صنعت نفت و گاز دولت هایی مانند عربستان یا ایران اختلال ایجاد کند و در نتیجه چنین اختلالی، سامانه حمل و نقل این کشور ها از کار بیفتد، چنین کاری باعث نارضایتی در حجم گسترده ای، به ویژه در کشوری مانند ایران، خواهد گردید (فرشا سعید پرویز و همکاران، 1401، ضرورت تقویت امنیت سایبری بخش انرژی توسط دولت ها). در ذیل به بعضی از اقدامات استعماری کشور های شمال و فناوری های وابسته به این کشور ها در عرصه تضعیف اقتصادی کشور های جنوب میپردازیم:

اول – فرار اطلاعات و درآمد دیجیتال: شرکت‌های بزرگ فناوری مانند گوگل، متا (فیسبوک) و آمازون، اطلاعات کاربران کشورهای جنوب را جمع‌آوری کرده، تحلیل می کنند و از طریق تبلیغات و فروش اطلاعات، درآمد هنگفتی کسب میکنند؛ در حالیکه این کشورها سهمی از این درآمد ندارند.

دوم – تضعیف کسب وکارهای محلی: پلتفرم‌های خارجی با قدرت سرمایه و دسترسی به اطلاعات، بازارهای آنلاین محلی را از رقابت خارج میکنند. به عنوان مثال، ورود پلتفرم‌های فروش بین‌المللی باعث شکست فروشگاه‌های اینترنتی بومی در بسیاری از کشورها شده است.

سوم – وابستگی فناوری و خروج ارز: کشورهایی که فاقد زیرساخت‌های فناوری هستند، ناچار به واردات نرم‌افزار، سخت افزار و خدمات از کشورهای شمال می باشند که این وابستگی باعث خروج گسترده ارز و تضعیف اقتصاد ملی میشود.

چهارم – بی‌عدالتی در مالیات دیجیتال: غول‌های فناوری در کشورهای جنوب فعالیت اقتصادی گسترده دارند اما به دلیل نبود قوانین مؤثر، مالیات اندکی می پردازند یا اصلاً مالیاتی پرداخت نمیکنند.

پنجم – مانع رشد اقتصاد دیجیتال بومی: تسلط کامل شرکت‌های خارجی بر فضای دیجیتال، فرصت‌های نوآوری و رشد برای شرکت‌های نوپای داخلی را محدود میکند، زیرا آن‌ها به اطلاعات، منابع و بازار دسترسی ندارند.

ب – تأثیر استعمار دیجیتال در بخش سیاست: فضای سایبر نماد برجسته ای از حیات مدرن جامعه بشری است. افراد و جوامع در سراسر جهان به وسیله فضای سایبر به یکدیگر متصل شده و ارتباط برقرار میکنند. این پیوند جامعه بشری به وسیله اینترنت، اگرچه باعث سرعت گردش اطلاعات و انجام شدن سریع کار ها گردیده، از جهتی دیگر دریچه های متعددی را برای سوء استفاده افراد و دولت ها گشوده است. رقابت و مسابقه ای که پیش از این در ساخت سلاح های کلاسیک وجود داشت، هم اکنون به این فضا کشیده شده و عرصه نوینی را برای رقابت دولت های ایجاد کرده است (فرشا سعید پرویز و همکاران، 1401، ضرورت تقویت امنیت سایبری بخش انرژی توسط دولت ها). امروزه حملات سایبری کشور های شمال به زیر ساخت های سایبری کشور های جنوب و به خصوص در امر حصول اهداف سیاسی فوق العاده گسترش پیدا نموده است که از آن جمله میتوان به انفجار پیجر های کاربردی اعضای حزب الله به لبنان اشاره کرد که در آن صد ها نفر شهید و هزاران نفر زخمی گردیدند که این طرح حمله سایبری توسط اسرائیل سال ها قبل طراحی گردیده بود. به همین ترتیب اسرائیل با همکاری غول های بزرگ فضای سایبر از قبیل، متا، گوگل وسایر پلتفورم ها توانست حملات مرگ باری را در غزه و سایر کشور های خاور میانه از جمله سوریه، لبنان، یمن و حتی ایران سازمان دهی نماید. این تنها اسرائیل نبود بلکه کشور های دیگر هم از قبیل بریتانیا و امریکا در زمینه وی را همکاری نمودند. از دیگر مثال های اینچنینی میتوان به حمله سایبری روسیه به استونی، گرجستان هم اشاره نمود، همچنان حملات بی وقفه امریکا به زیر ساخت های ایران به منظور حصول اهداف سیاسی از دیگر نمونه این استعمار دیجیتالی در عرصه سیاست و حصول مقاصد سیاسی میباشد. در مجموع این حملات عمدا در قبال کشور های جنوب توسط کشور های شمال سازماندهی میگردد. در کل میگویم که استعمار دیجیتال به معنای تسلط شرکت‌های فناوری بزرگ (*Big Tech*) بر زیرساخت‌ها، اطلاعات و سیاست‌های دیجیتال کشورهای جنوب جهانی است. این تسلط، حاکمیت ملی را تضعیف کرده و فرآیندهای سیاسی را تحت تأثیر قرار میدهد. این اثر گذاری های استعمار دیجیتالی در عرصه سیاست را ذیلا به طور شماره وار اشاره میدارم:

الف – تضعیف حاکمیت دیجیتال؛

ب – نفوذ در سیاست گذاری ها؛

ج – تغییر در ساختارهای حکمرانی؛

د – نقض حریم خصوصی و نظارت گسترده؛

هـ – محدودیت در توسعه فناوری بومی؛

ج – تأثیر استعمار دیجیتال در بخش امنیت: در گذشته، امنیت بیشتر به صورت ملی و در داخل مرزهای کشورها تعریف میشد و دولت‌ها با ایجاد نهادهایی مانند اردو و سازمان‌های اطلاعاتی، امنیت داخلی را تأمین میکردند. اما با گسترش سلاح‌های پیشرفته و تهدیدهای جهانی، مفهوم امنیت تغییر کرد و سازمان‌های بین‌المللی برای حفظ صلح به وجود آمدند. با ظهور اینترنت و فناوری‌های نو، تهدیدهای سایبری نیز مطرح شد که مرزها را بی معنا ساخت. امروزه هر فردی می تواند با استفاده از فضای مجازی به دیگران آسیب برساند، بنابراین امنیت تنها یک مسئله ملی نیست، بلکه به یک موضوع جهانی و فردی تبدیل شده است. در گذشته، امنیت بیشتر مفهومی ملی داشت و دولت‌ها در چارچوب مرزهای خود به آن می

پرداختند. با گسترش سلاح‌های پیشرفته، مفهوم امنیت جهانی شد و سازمان‌هایی مانند سازمان ملل و ناتو برای حفظ صلح شکل گرفتند. اما با ظهور فناوری‌های سایبری، امنیت ابعاد جدیدی پیدا کرد؛ زیرا تهدیدات سایبری مرز نمی شناسند و میتوانند با کمترین هزینه، خسارات بزرگی ایجاد کنند. در نتیجه، امنیت ملی به امنیت بین‌المللی تبدیل شده و نیاز به همکاری جهانی در این حوزه بیشتر از گذشته احساس می شود (فرشا سعید پرویز و همکارن، 1401، ضرورت همکاری دولت ها در تقویت امنیت سایبری).

استعمار دیجیتال به معنای تسلط شرکت‌ها و قدرت‌های فناوری بر زیرساخت‌ها، اطلاعات و سیاست‌های دیجیتال کشورهای دیگر است. این تسلط میتواند تأثیرات قابل توجهی بر بخش امنیتی کشورها، به ویژه کشورهای جنوب جهانی، داشته باشد. در ادامه، به برخی از این تأثیرات اشاره می‌شود:

الف – تضعیف حاکمیت دیجیتال: وابستگی به فناوری‌ها و زیرساخت‌های دیجیتال خارجی میتواند حاکمیت دیجیتال کشورها را تضعیف کند. زمانی که داده‌ها و اطلاعات حساس در اختیار شرکت‌ها یا دولت‌های خارجی قرار میگیرد، امکان سوء استفاده یا اعمال نفوذ وجود دارد که این امر فوق العاده شکننده بوده و امنیت کشور را دچار تهدیدات فزاینده میسازد.

ب – افزایش آسیب پذیری در برابر حملات سایبری: استفاده از نرم افزارها و سخت افزارهای وارداتی ممکن است دربردارنده آسیب پذیری‌هایی باشد که توسط تولید کنندگان یا دولت‌های پشتیبان آن‌ها قابل بهره برداری است مانند پیجر های اعضای حزب الله در لبنان. این امر می تواند امنیت ملی را به خطر انداخته و اضرار غیر قابل جبران را به بار آورد.

ج – نقض حریم خصوصی و نظارت گسترده: شرکت‌های فناوری با جمع آوری اطلاعات کاربران، می توانند نظارت گسترده ای بر فعالیت‌های آن‌ها داشته باشند. این نظارت میتواند برای کنترل سیاسی، اجتماعی و امنیتی مورد استفاده قرار گیرد و نیزحریم خصوصی افراد را نقض کرده و از طریق این نقض حریم خصوصی، موضوع باج گیری مطرح شده و موضوع امینت کشور موضوع آن باج گیری قرار گرفته و به خطر مواجه شود.

د – تأثیر بر سیاست گذاری‌های امنیتی: وابستگی به فناوری‌های خارجی ممکن است بر سیاست گذاری‌های امنیتی کشورها تأثیرگذار باشد. کشورها ممکن است در تدوین سیاست‌های امنیتی خود مجبور به تبعیت از استانداردها و قوانین کشورهای تولید کننده فناوری شوند.

هـ – محدودیت در توسعه فناوری بومی: تسلط شرکت‌های فناوری خارجی بر بازارهای دیجیتال میتواند فرصت‌های توسعه فناوری بومی را محدود کند. این امر منجر به وابستگی بیشتر کشورها به فناوری‌های خارجی میشود و توانمندی‌های داخلی را تضعیف میکند. این امر نیز بر سیاست های امنیتی کشور تأثیرات ناگواری را وارد میکند.

در مجموع، استعمار دیجیتال می تواند تهدیدات جدی برای امنیت ملی و حاکمیت دیجیتال کشورها ایجاد کند. برای مقابله با این تهدیدات، توسعه فناوری‌های بومی، تدوین سیاست‌های مستقل دیجیتال و همکاری‌های منطقه ای و بین‌المللی ضروری است.

د – تأثیر استعمار دیجیتال در بخش فرهنگ: با گسترش و کاربرد شبکه های اجتماعی از قبیل: فیسبوک، یوتیوب، انستاگرام، تیک تاک وغیره. فرهنگ ملت ها دچار حملات بی سابقه این ابزار های سایبری قرار گرفته و عملا در معرض نابودی قرار گرفته اند. امروزه مردم در جوامع مختلف و به خصوص جوامع شرقی و کشور های جنوب جهانی در خلاء بی هوئیتی

فرهنگی قرار گرفته و روز به روز جوانان از فرهنگ خویش بیگانه شده و فرهنگ غربی را جای گزین فرهنگی بومی و ملی خویش میسازند.

استعمار دیجیتال به معنای تسلط شرکت‌ها و قدرت‌های فناوری بر زیرساخت‌ها، اطلاعات و سیاست‌های دیجیتال کشورهای دیگر است. این تسلط میتواند تأثیرات قابل توجهی بر بخش فرهنگی کشورها، به ویژه کشورهای جنوب جهانی، داشته باشد. در ادامه، به برخی از این تأثیرات اشاره میشود:

الف – تضعیف تنوع فرهنگی و هویت‌های محلی: شرکت‌های بزرگ فناوری با ارائه محتوای غالباً غربی، به تدریج فرهنگ‌ها و هویت‌های محلی را تحت تأثیر قرار میدهند. این روند میتواند منجر به کاهش تنوع فرهنگی و تضعیف ارزشها و سنت‌های بومی شود.

ب – وابستگی به زیرساخت‌ها و پلتفرم‌های خارجی: کشورهای جنوب برای دسترسی به خدمات دیجیتال، به زیرساخت‌ها و پلتفرم‌های شرکت‌های خارجی وابسته هستند. این وابستگی میتواند کنترل فرهنگی را از دست دولت‌ها خارج کرده و آن را در اختیار شرکت‌های خارجی قرار دهد.

ج – تسلط الگوریتم‌ها و اطلاعات غربی بر تولید محتوا: الگوریتم‌های هوش مصنوعی که بر اساس اطلاعات غربی آموزش دیده اند، ممکن است محتوای فرهنگی کشورهای جنوب جهانی را نادیده بگیرند یا به درستی نمایش ندهند. این موضوع میتواند به حاشیه نشینی فرهنگ‌های محلی در فضای دیجیتال منجر شود.

د – تأثیر بر زبان و ارتباطات فرهنگی: استفاده گسترده از زبان‌های غالب در پلتفرم‌های دیجیتال میتواند به تضعیف زبان‌های محلی و کاهش استفاده از آن‌ها در فضای دیجیتال منجر شود. این روند ممکن است به کاهش ارتباطات فرهنگی بومی و تضعیف هویت زبانی منجر شود.

هـ – تضعیف رسانه های محلی و صنایع فرهنگی: تسلط شرکت‌های بزرگ فناوری بر بازارهای تبلیغاتی و رسانه میتواند به کاهش درآمد و تأثیرگذاری رسانه ها و صنایع فرهنگی محلی منجر شود. این موضوع ممکن است به کاهش تولید محتوای فرهنگی بومی و وابستگی بیشتر به محتوای خارجی منجر شود.

3 – نمونه هایی از سلطه پلتفرم های بزرگ بر اطلاعات کشور های جنوب: قبل از اینکه به این نمونه ها بپردازیم، لازم میدانم مختصرا به استفاده حد اکثری از شبکه های سایبری در یک دهه پسین اشاره داشته باشم. در سال 2015م پانزده ملیارد دستگاه به انترنت وصل بود و این رقم در سال 2025م به 75 ملیارد میرسد. اکثریت این دستگاه ها را موبایل های هوشمند تشکیل میدهد. بنابر قابلیت های موبایل های هوشمند، برقراری ارتباط در فضای سایبر و رد وبدل کردن اطلاعات، جهان را به یک شهر کوچک تبدیل کرده است. بنا فضای سایبر پر از تهدید و سهولت برای اعضای آن است. امروزه موبایل و کمپیوتر مردم پر از عکس، فیلم، صوت و دیگر اطلاعات خصوصی است که مجرمین می توانند به سهولت به آن دست برد بزنند (حسینی سید محمد و هاشمی غاز، 1398، حقوق جزای اختصاصی 3). بنا مجرمین به طریق اولی میتوانند که اطلاعات شخصی و دولتی کشور های جنوب را که کمتر با قابلیت های فضای سایبر آشنائی دارند بدوزدند و از آن به نفع خویش و کشور های شمال استفاده به عمل آورند. اکنون در ذیل به چند نمونه از نمونه های مهم غول های بزرگ قدرت های شمال برکسب اطلاعات کشور های جنوب میپردازیم:

الف – پروژه *Free Basics* فیسبوک یا *was a partnership with cellular network* (این پروژه یک بخش از کمپنی امروزی *Meta* که در گذشته برایش *Facebook* نامیده میشد): فیسبوک در سال ۲۰۱۵ پروژه ای به نام *Free Basics* را راه اندازی کرد که به کاربران در کشورهای در حال توسعه امکان دسترسی رایگان به بخش‌هایی از اینترنت را میداد. این پروژه با انتقادات فراوانی مواجه شد، زیرا به فیسبوک کنترل بیشتری بر تجربه اینترنتی کاربران میداد و به نقض بیطرفی شبکه متهم شد. در هند، این پروژه به دلیل اعتراضات گسترده ممنوع شد، اما در بیش از ٦٠ کشور دیگر، از جمله کنیا و غنا، همچنان فعال است.

ب – تسلط گوگل و فیسبوک بر تبلیغات آنلاین در آفریقای جنوبی: در آفریقای جنوبی، گوگل و فیسبوک بخش عمده ای از بازار تبلیغات آنلاین را در اختیار دارند، که تهدیدی جدی برای رسانه‌های محلی محسوب میشود. این تسلط باعث کاهش درآمد رسانه‌های بومی و تضعیف آن‌ها در رقابت با غول‌های فناوری شده است.

ج – جمع آوری اطلاعات کاربران توسط گوگل: گوگل از طریق خدمات مختلفی مانند جستجو، نقشه ها، تبلیغات، سیستم‌عامل اندروید و جیمیل، اطلاعات گسترده ای از کاربران جمع آوری میکند. این اطلاعات به سرورهای شرکت منتقل شده و برای ارائه خدمات و کسب درآمد استفاده میشوند، در حالی که کشورهای مبدأ کنترل کمی بر این داده‌ها دارند.

د – موقعیت مراکز اطلاعات فیسبوک: با وجود اینکه کشورهایی مانند هند بیشترین تعداد کاربران فیسبوک را دارند، اکثر مراکز اطلاعات این شرکت در آمریکای شمالی و اروپا واقع شده اند. این موضوع نگرانی هایی درباره حاکمیت اطلاعات و بهره برداری از اطلاعات کاربران کشورهای در حال توسعه ایجاد کرده است.

هـ – نفوذ شرکت‌های فناوری در نظام آموزشی آفریقای جنوبی: شرکت‌هایی مانند مایکروسافت و گوگل با ارائه نرم‌افزارها و خدمات آموزشی، نفوذ گسترده‌ای در نظام آموزشی آفریقای جنوبی پیدا کرده اند. این شرکت‌ها با ارائه ابزارهای آموزشی و جمع‌آوری اطلاعات متعلمین، کنترل بیشتری بر اطلاعات آموزشی و فرهنگی این کشورها به دست آورده اند(*Longreads .tni.org/digital-colonialism-the-evolution-of-us-empire?utm_source=chatgpt.com longreads*). این نمونه‌ها نشان دهنده چگونگی تسلط پلتفرم‌های بزرگ فناوری بر اطلاعات و زیرساخت‌های دیجیتال کشورهای جهان سوم هستند. برای مقابله با این روند، توسعه زیرساخت‌های دیجیتال بومی، تدوین سیاست‌های مستقل اطلاعاتی و همکاری‌های منطقه ای ضروری است.

مبحث چهارم – آسیب پذیری و وابستگی کشور های جنوب:

کشورهای جنوب جهانی (*Global South*) شامل بسیاری از کشورهای آسیایی، آفریقایی و آمریکای لاتین اند که با چالش‌های جدی در حوزه استقلال سایبری و دیجیتال روبه رو هستند. این چالش‌ها شامل موارد زیر میباشند:

الف – نبود زیرساخت‌های بومی سایبری: بسیاری از کشورهای جنوب فاقد زیرساخت‌های سخت افزاری و نرم افزاری بومی برای حفاظت از فضای سایبری خود هستند. این مسئله باعث میشود تا برای فعالیت‌های دیجیتال، به زیرساخت‌های وارداتی و خارجی وابسته باشند. این وابستگی میتواند باعث از دست دادن کنترل دولت‌ها بر اطلاعات و معلومات حیاتی کشورها شده و در مواقع بحرانی امنیت ملی تهدید شود. به‌عنوان‌مثال، بحران‌های سیاسی یا اجتماعی میتوانند به راحتی توسط نیروهای خارجی یا از طریق پلتفرم‌های جهانی دستکاری شوند.

ب – وابستگی به فناوری‌ها، نرم افزارها و سرورهای خارجی: این کشورها عمدتاً از سیستم‌عامل‌ها، اپلیکیشن‌ها، ابزارهای امنیتی، سرورهای ابری و نرم افزارهایی استفاده میکنند که متعلق به شرکت‌های بزرگ فناوری در ایالات متحده، اروپا یا چین هستند. این وابستگی نه تنها امنیت اطلاعات را تهدید میکند، بلکه حاکمیت ملی دیجیتال را نیز تضعیف میسازد. در سال‌های اخیر، حملات سایبری به زیرساخت‌های دولت‌ها در کشورهای آفریقایی و آسیایی گزارش شده است. این حملات نه تنها به سیستم‌های دولتی آسیب می زنند بلکه میتوانند پیامدهایی در بخش‌های اقتصادی و اجتماعی ایجاد کنند. به‌عنوان مثال، حمله به سیستم‌های مالی یا انرژی میتواند بحران‌های گسترده ای ایجاد کند.

ج – ناتوانی در تولید سیستم‌عامل‌ها، دیتابیس‌ها و خدمات ابری: تولید فناوری‌های پیچیده مانند سیستم‌عامل‌های ملی، بانک‌های اطلاعاتی و خدمات ابری نیازمند منابع مالی، انسانی و فنی گسترده است که اغلب در کشورهای جنوب فراهم نیست. این ناتوانی موجب میشود اطلاعات حساس این کشورها در سرورهای خارجی ذخیره شود و امکان سوء استفاده و کنترل از بیرون را فراهم سازد. این امر ممکن است به نقض حریم خصوصی شهروندان کشورهای جنوب منجر شود و دولت‌ها را در موقعیت ضعیفی در مقابل فشارهای خارجی قرار دهد. به طور خاص، کشورهایی که از فناوری‌های داخلی خود برای محافظت از اطلاعات استفاده نمیکنند، به راحتی در معرض کنترل و نفوذ کشورهای پیشرفته قرار دارند. بررسی مثال‌هایی از کشورهای آمریکای لاتین، آفریقا و آسیا.

برزیل: پس از افشای جاسوسی سایبری آمریکا (*NSA*)، این کشور اقدام به توسعه زیرساخت‌های بومی کرد اما هنوز در بسیاری از بخش‌ها به پلتفرم‌های خارجی وابسته است.

نیجریه: به شدت وابسته به خدمات ابری خارجی مانند *AWS* و *Google Cloud* است و توانمندی اندکی در تولید نرم افزارهای امنیتی بومی دارد.

د – خطرات و آسیب‌های اجتماعی و سیاسی: استعمار دیجیتال میتواند تأثیرات منفی زیادی بر امنیت اجتماعی و سیاسی کشورهای جنوب جهانی بگذارد. به ویژه در هنگام استفاده از رسانه های اجتماعی و شبکه‌های اینترنتی، بسیاری از اطلاعات میتوانند به صورت نادرست یا تحریف شده منتشر شوند که این میتواند به ناآرامی‌های اجتماعی و سیاسی در کشورهای جنوب منجر شود.

به‌عنوان مثال، در کشورهای آفریقایی یا آسیایی، گاهی اوقات دولت‌ها از دسترسی به شبکه‌های اجتماعی یا مسدودسازی اطلاعات به‌عنوان یک ابزار کنترل استفاده میکنند که این امر خود میتواند به بحران‌های اجتماعی دامن بزند. یا هم در افغانستان در ایام خاص مثل اعیاد دولت همه شبکه ها را برای حد اقل شش ساعت مسدود میسازد.

هـ – آسیب‌های اقتصادی و وابستگی به بازارهای جهانی: یکی دیگر از آثار استعمار دیجیتال، تأثیر آن بر بخش اقتصادی کشورهای جنوب جهانی است. بسیاری از این کشورها به دلیل استفاده از پلتفرم‌های دیجیتال و خدمات ابری که توسط شرکت‌های خارجی ارائه میشود، وابسته به بازارهای جهانی هستند. این وابستگی متواند به کاهش کنترل داخلی بر اقتصاد ملی منجر شود، چرا که کشورهای جنوب ممکن است توانایی توسعه فناوری‌های بومی خود را از دست بدهند و در پی آن، واردات و هزینه‌های اقتصادی آن‌ها افزایش یابد.

و – نقش پلتفرم‌های جهانی در تغییرات فرهنگی و اجتماعی: استعمار دیجیتال در بسیاری از مواقع از طریق پلتفرم‌های رسانه ای و شبکه‌های اجتماعی موجب تغییرات فرهنگی و اجتماعی در کشورهای جنوب جهانی میشود. این پلتفرم‌ها

میتوانند روندهای فرهنگی و اجتماعی را تحت تأثیر قرار دهند و هنجارها و الگوهای رفتاری جدیدی را معرفی کنند که ممکن است با فرهنگ و سنت‌های بومی آن کشورها تضاد داشته باشد. بسیاری از محتوای منتشر شده در رسانه‌های اجتماعی به ویژه در کشورهای در حال توسعه، تحت تأثیر فرهنگ غربی است که به طور غیرمستقیم فرهنگ محلی این کشورها را تحت‌الشعاع قرار میدهد. این امر ممکن است منجر به از دست دادن هویت فرهنگی و ایجاد یک فرهنگ جهانی تحمیل شده شود (*https://peivast.com/p/218105](https://peivast.com/p/218105*).

مبحث پنجم – قدرت های شمال و سلطه سایبری

قدرت‌های شمال، به خصوص امریکا، اتحادیه اروپا، چین و روسیه، در دنیای دیجیتال نقش تعیین کننده ای دارند و به طور فزاینده ای از ابزارهای سایبری برای گسترش نفوذ خود استفاده میکنند. این کشورها با بهره برداری از زیرساخت‌های دیجیتال و داده‌ها، قدرت نرم و سخت خود را در سطوح جهانی اعمال میکنند. از یک سو، تسلط بر فناوری‌های سایبری به آن‌ها این امکان را میدهد که در سیاستگذاری جهانی تاثیرگذار باشند، و از سوی دیگر، با استفاده از حملات سایبری و جاسوسی اطلاعاتی، میتوانند تهدیدات جدیدی برای امنیت جهانی ایجاد کنند.

1 – قدرت های شمال در زمینه فضای سایبر: در ذیل به قدرت های شمال و نقش اعمال قدرت سایبری هر یک از این قدرت ها میپردازیم:

الف – ایالات متحده امریکا: ایالات متحده امریکا یکی از پیشگامان در زمینه فناوری و امنیت سایبری است و نقش کلیدی در ایجاد استانداردهای بین‌المللی برای فضای سایبری ایفا میکند مانند *ISO* و *NIS*. با توجه به حجم عظیم اطلاعات جمع‌آوری شده توسط دولت‌ها و شرکت‌های خصوصی، ایالات متحده از قدرت سایبری خود برای اعمال تأثیر بر سیاست‌ها و اقتصاد جهانی استفاده می‌کند. برای مثال، ایالات متحده در ایجاد و توسعه سیستم‌های اطلاعاتی نظیر گوگل، فیسبوک، آمازون و سایر پلتفرم‌ها نقش برجسته ای دارد. همچنین در زمینه جاسوسی سایبری، آژانس امنیت ملی (*NSA*) ایالات متحده از ابزارهایی برای جمع آوری اطلاعات از سراسر جهان استفاده میکند (*Reuters. "China accuses US of launching 'advanced' cyberattacks, names alleged NSA agents." April 15, 2025*).

ب – اتحادیه اروپا: اتحادیه اروپا تلاش دارد تا در زمینه حاکمیت دیجیتال و فضای سایبری امنیت بیشتری برقرار کند. سیاست‌هایی مانند *GDPR* یا *General Data Protection Regulation* (قانون حفاظت از اطلاعات عمومی است برای نگهداری معلومات اتحادیه اروپا) به طور خاص برای محافظت از داده‌های شخصی و مقابله با نفوذ خارجی بر فضای سایبری ایجاد شده است. اتحادیه اروپا به ویژه در مقابله با تهدیدات سایبری خارجی و تأمین امنیت فضای دیجیتال در برابر حملات و مداخلات خارجی فعال است (*European Commission. "General Data Protection Regulation (GDPR)*).

ج – چین: چین به طور فزاینده ای به یک قدرت سایبری در عرصه جهانی تبدیل شده است. با برنامه‌هایی مانند طرح "چین 2025" که به دنبال تقویت فناوری‌های نوین از جمله *G5* و اینترنت اشیاء است، چین برای بهبود قدرت سایبری خود سرمایه گذاری میکند. چین همچنین در زمینه امنیت سایبری در داخل کشور نظارت شدیدی بر اطلاعات و شبکه‌ها دارد و کنترل دقیقی بر فضای اینترنت در داخل کشور اعمال میکند. در سطح جهانی، چین از قابلیت‌های سایبری خود برای جمع‌آوری اطلاعات و حتی اعمال نفوذ در سیاست‌های کشورهای دیگر استفاده میکند.

د – روسیه: روسیه یکی از بازیگران اصلی در حوزه امنیت سایبری و مداخلات دیجیتال است. این کشور به ویژه در زمینه حملات سایبری به زیرساخت‌های کشورهای غربی شناخته شده است. در انتخابات مختلف، به ویژه انتخابات ریاست جمهوری ایالات متحده در سال ۲۰۱٦، روسیه به طور گسترده به اتهام مداخله در سیاست‌های کشورهای خارجی از جمله به کشور اکراین متهم شده است. روسیه همچنین از توانایی‌های سایبری خود برای ایجاد اختلال در انتخابات و حملات اطلاعاتی استفاده کرده است (*Time. "Here's The Evidence Russia Hacked The Democratic National (Committee."* - *December 14, 2016*).

2 – استفاده اطلاعات برای اعمال قدرت نرم و سخت: در ذیل مختصرا به قدرت نرم و سخت اشاره مختصر میداشته باشیم:

الف – قدرت نرم: قدرت نرم به استفاده از منابع غیرمستقیم مانند فرهنگ، ایده‌ها، رسانه‌ها و شبکه‌ها برای تأثیرگذاری بر افکار عمومی و سیاست‌های خارجی کشورهای دیگر اطلاق میشود. استفاده از داده‌ها در این حوزه میتواند شامل دستکاری در اطلاعات، تحلیل‌های پیش‌بینی پذیر از رفتارهای اجتماعی و اقتصادی و حتی تبلیغات سیاسی باشد. برای مثال، استفاده از اطلاعات کاربران در پلتفرم‌های اجتماعی (مانند فیسبوک و توییتر) میتواند برای تأثیرگذاری بر انتخابات، تشکیل گروه‌های اجتماعی و تغییر در نگرش‌های عمومی مورد استفاده قرار گیرد. ایالات متحده و اتحادیه اروپا در زمینه تحلیل داده‌های جمع‌آوری‌شده برای اعمال قدرت نرم در عرصه جهانی فعال بوده اند (*Wikipedia. "Facebook–Cambridge Analytica data scandal*).

ب – قدرت سخت: قدرت سخت به استفاده از ابزارهای نظامی و اقتصادی برای اعمال تأثیر بر کشورها اشاره دارد. در دنیای سایبری، این به معنای استفاده از حملات سایبری و جاسوسی اطلاعاتی برای آسیب رساندن به زیرساخت‌ها و نفوذ در سیستم‌های حساس است. کشورهای بزرگی مانند ایالات متحده و روسیه از توانایی‌های سایبری خود برای ایجاد اختلال در فعالیت‌های دولتی و اقتصادی کشورها بهره برداری کرده‌اند (*Wikipedia. "Fancy Bear*).

3 – مداخلات سایبری و جاسوسی اطلاعاتی: ذیلا از مداخلات سایبری و جاسوسی قدرت های شمال تذکر مختصر به عمل میآوریم:

الف – مداخلات سایبری: این نوع مداخلات میتواند شامل حملات به سرورهای دولتی، حذف یا تغییر اطلاعات حیاتی، تضعیف اعتماد عمومی و در نهایت ایجاد اختلال در فرایندهای سیاسی و اقتصادی باشد. یکی از معروف ترین نمونه‌ها حملات سایبری به سیستم‌های انتخابات در ایالات متحده و سایر کشورهای غربی است (*https://www.npr.org/2020/02/12/805498673/russian-interference-in-2016-us-election-what-you-need-to-know?utm_source=chatgpt.com*).

ب – جاسوسی: جاسوسی سایبری شامل دسترسی غیرمجاز به اطلاعات محرمانه است که به منظور جمع‌آوری اطلاعات اقتصادی، نظامی یا سیاسی از کشورهای دیگر انجام میشود. این عملیات‌ها اغلب توسط آژانس‌های امنیت ملی کشورهای قدرتمند مانند *NSA* در ایالات متحده و *FSB* در روسیه انجام میشود (*The National Security Agency's (NSA) Surveillance Programs*).

مبحث ششم – پیامد های وابستیگی سایبری

وابستگی به فناوری‌های سایبری، به ویژه در کشورهایی که زیرساخت‌های دیجیتال آن‌ها وابسته به قدرت‌های خارجی است، پیامدهای قابل توجهی به همراه دارد. این وابستگی میتواند تهدیدهایی همچون آسیب به حاکمیت ملی، اختلال در خدمات حیاتی، بحران اعتماد عمومی و نشت اطلاعات شخصی کاربران را ایجاد کند. همچنین، وابستگی اقتصادی به شرکت‌های چندملیتی فناوری، کشورهای وابسته را در معرض سلطه خارجی و آسیب‌های اقتصادی قرار میدهد. بنابراین، این پیامدها نیازمند توجه جدی و استراتژی‌های مؤثر برای مدیریت تهدیدات سایبری است.

1 – تهدید حاکمیت ملی و امنیت اطلاعات: وابستگی سایبری می‌تواند تهدیدی جدی برای حاکمیت ملی کشورها باشد، به خصوص وقتی که کشورهای وابسته به فناوری‌های خارجی قادر به مدیریت و حفاظت از اطلاعات حساس خود نیستند. در این زمینه، تهدیدات امنیتی از طریق هک، جاسوسی سایبری، یا حملات سایبری به بخش‌های حیاتی دولت‌ها و سازمان‌ها به شدت افزایش می یابد. کشورهایی که وابسته به قدرت‌های خارجی در زمینه زیرساخت‌های سایبری هستند، در صورت بروز مشکلات امنیتی، به طور مستقیم تحت تأثیر این تهدیدات قرار خواهند گرفت (*Craig, A. M. (2017). Cybersecurity and National Sovereignty: A Global Perspective. Journal of Information Warfare, 16(3), 78-91*).

2 – اختلال در خدمات حیاتی در صورت قطع ارتباط: خدمات حیاتی همچون شبکه‌های برق، سیستم های صحت، حمل و نقل و خدمات دولتی به شدت به زیرساخت‌های سایبری وابسته هستند. در صورت قطع ارتباطات اینترنتی یا حملات سایبری به این سیستم‌ها، ممکن است اختلالات گسترده ای در ارائه این خدمات ایجاد شود که عواقب اجتماعی و اقتصادی زیادی به دنبال خواهد داشت. این نوع وابستگی سایبری میتواند در مواقع بحرانی کشورها را در وضعیت آسیب پذیری قرار دهد (*Smith, D. L., & Petersen, M. (2019). The Impact of Cyberattacks on Critical Infrastructure. International Journal of Cyber Security, 14(4), 132-145*).

3 – بحران اعتماد عمومی و نشت اطلاعات کاربران: یکی از پیامدهای وابستگی سایبری، بحران اعتماد عمومی به سیستم‌های اطلاعاتی است. هنگامی که اطلاعات حساس کاربران از طریق داده‌های نشت شده یا حملات سایبری منتشر میشود، اعتماد مردم به نهادهای دولتی و خصوصی در حفظ امنیت اطلاعات آسیب میبینند. نشت اطلاعات کاربران یا سوء استفاده از اطلاعات شخصی میتواند به بروز بحران‌های اجتماعی و سیاسی منجر شود (*Kaspersky, A. (2020). Data Breaches and Public Trust: The Need for Better Cybersecurity. Journal of Information Privacy, 18(2), 99-110*).

4 - وابستگی اقتصادی به شرکت‌های چند ملیتی فناوری: وابستگی سایبری همچنین وابستگی اقتصادی به شرکت‌های فناوری بزرگ مانند گوگل، مایکروسافت، اپل و آمازون را ایجاد میکند. این شرکت‌ها غالباً کنترل زیادی بر روی زیرساخت‌های دیجیتال و فضای ابری دارند و کشورها برای مدیریت اقتصاد دیجیتال خود به این شرکت‌ها وابسته هستند. در چنین وضعیتی، این شرکت‌ها میتوانند سیاست‌های خود را به عنوان قدرت اقتصادی و فناوری در جهان تحمیل کنند و کشورها را در موقعیتی آسیب پذیر قرار دهند (*Fisher, S. L., & Andrews, D. (2018). The Economic Consequences of Cyber Dependency on Multinational Tech Companies. Global Economic Review, 25(1), 45-60*).

در مجموع پیامدهای وابستگی سایبری کشورها به فناوری‌های خارجی میتواند تهدیدات جدی برای امنیت ملی، اقتصادی و اجتماعی آن‌ها به همراه داشته باشد. از تهدیدات امنیتی گرفته تا بحران‌های اعتماد عمومی و اختلال در خدمات حیاتی، وابستگی به پلتفرم‌ها و شرکت‌های چندملیتی میتواند منجر به آسیب پذیری‌های گسترده ای شود که لازم است کشورها برای مقابله با آن‌ها استراتژی‌های دقیق و مؤثری اتخاذ کنند.

مبحث هفتم – راهبرد های مقابله با استعمار دجیتال

راهبردهای مقابله با استعمار دیجیتال مجموعه ای از سیاست‌ها و اقدامات هدفمند برای حفظ حاکمیت سایبری و کاهش وابستگی به قدرت‌های فناورانه شمال جهانی است. در عصر تسلط فناوری‌های نوین اطلاعاتی، کشورهای جنوب با چالش‌های جدی در زمینه وابستگی به زیرساخت‌ها، نرم‌افزارها و اطلاعات مواجه اند. از این رو، تقویت امنیت سایبری ملی، توسعه فناوری بومی، همکاری‌های منطقه‌ای جنوب – جنوب و شکل دهی به قواعد حقوقی بین المللی، از مهمترین اقدامات برای مقابله با این پدیده هستند. این راهبردها نقش کلیدی در حفاظت از استقلال دیجیتال و صیانت از منافع ملی ایفا میکنند که در ذیل به چند نمونه آن میپردازیم:

1 – سیاست‌های امنیت سایبری ملی: تدوین و اجرای سیاست‌های امنیت سایبری ملی، یکی از راهبردهای اساسی در مقابله با استعمار دیجیتال است. این سیاست‌ها با هدف حفظ حاکمیت دیجیتال و مقابله با تهدیدات سایبری طراحی میشوند. برای مثال، تدوین چرخه عمر استراتژی ملی امنیت سایبری در ایران، شامل مراحل مختلفی از جمله ارزیابی و تحلیل، تدوین استراتژی، اجرا و نظارت است که به تقویت امنیت سایبری کشور کمک میکند (*IRNA* *./www.irna.ir/news/84065810*).

2 – تولید دانش بومی و توسعه فناوری داخلی: توسعه فناوری‌های بومی و تولید دانش داخلی، نقش مهمی در کاهش وابستگی به فناوری‌های خارجی دارد. برای نمونه، در ایران، پروژه‌هایی مانند بومی سازی آنتی ویروس و ایجاد مرکز مدیریت امنیت (*SOC*) توسط پژوهشگاه ارتباطات و فناوری اطلاعات انجام شده است. این اقدامات با هدف تقویت توانمندی‌های داخلی در حوزه امنیت سایبری و کاهش وابستگی به محصولات خارجی صورت گرفته اند.

3 – همکاری‌های منطقه ای جنوب – جنوب: تقویت همکاری‌های منطقه ای میان کشورهای جنوب جهانی، میتواند به تبادل تجربیات و منابع در حوزه فناوری اطلاعات و امنیت سایبری منجر شود. برای مثال، پیوستن افغانستان به اتحادیه همکاری‌های منطقه ای جنوب آسیا (*SAARC*)، فرصتی برای همکاری‌های بیشتر در زمینه‌های مختلف از جمله فناوری و امنیت سایبری فراهم کرده است (صدای آمریکا:- *ir.voanews.com/a/a-31-2007-04-03-voa1*).

4 – توسعه قوانین بین‌المللی برای کنترل قدرت‌های سایبری: تدوین و اجرای قوانین بین‌المللی در حوزه فضای سایبری، برای مقابله با تهدیدات ناشی از قدرت‌های سایبری ضروری است. کنوانسیون بوداپست و دستورالعمل تالین، از جمله اسناد بین‌المللی هستند که به تعیین چارچوب‌های قانونی برای مقابله با جرائم سایبری و حفظ امنیت در فضای مجازی کمک میکنند. این اسناد با ایجاد سازوکارهای همکاری بین‌المللی و تعیین مجازات‌های مناسب، نقش مهمی در مقابله با تهدیدات سایبری ایفا میکنند (*aftana.ir:* www.aftana.ir/article/22632?utm_source=chatgpt.com).

5 – ایجاد تیم های *CSIR* یعنی سیستم های مقابل حملات سایبری در صورت وارد عمل شوند. که به شکل پدافند در مقابل آفند عمل میکنند.

6 – ایجاد وسایل الکترونیکی مستقل مانند: *Reuter*، *Server* وغیره.

مبحث هشتم – پیشنهادات و راهکار ها

در ذیل، پیشنهادات و راهکارها برای مقابله با وابستگی سایبری و کاهش اثرات استعمار دیجیتال بر کشورهای جنوب جهانی، به صورت شماره وار ارائه میگردد:

1. تدوین استراتژی ملی امنیت سایبری: ایجاد سیاست جامع امنیت سایبری با هدف محافظت از زیرساخت‌های حیاتی، اطلاعات دولتی و داده‌های شهروندان توسط کشور های در حال توسعه و کشور های جنوب.
2. توسعه زیرساخت‌های بومی سایبری: سرمایه گذاری کشور های جنوب در ایجاد دیتاسنترها، شبکه های مستقل، و خدمات ابری بومی برای کاهش وابستگی به سرورهای خارجی و در مجموع قدرت های شمال.
3. توانمند سازی متخصصان داخلی: آموزش نیروی انسانی متخصص در حوزه تخنیک اطلاعات، امنیت سایبری، رمزنگاری، تحلیل داده ها وغیره توسط کشور های جنوب.
4. حمایت از تولید نرم افزارها و سیستم‌عامل‌های بومی: تولید و گسترش ابزارهای نرم افزاری ملی به ویژه در زمینه مرورگرها، پیام رسان ها و سیستم‌های مدیریت اطلاعات.
5. توسعه همکاری‌های منطقه ای جنوب – جنوب: ایجاد اتحادیه های فناوری و تخنیکی بین کشورهای جنوب برای اشتراک دانش، تجربیات و توسعه مشترک ابزارهای دیجیتال. در هر عصر و زمان برای رفع مشکلات وابستگی های سایبری.
6. ایجاد مراکز تحقیقاتی مستقل در حوزه سایبری: تأسیس مراکز علمی برای تحلیل تهدیدات سایبری، ردیابی حملات و ارائه راهکارهای علمی.
7. تقویت چارچوب های قانونی و حقوقی سایبری: وضع قوانین مشخص برای حفظ حریم خصوصی، مقابله با جرایم سایبری و تحدید فعالیت پلتفرم‌های خارجی بدون نظارت ملی.
8. کاهش وابستگی به شرکت‌های فناوری چندملیتی: توسعه فناوری‌های جایگزین داخلی برای محصولات شرکت‌هایی مانند *Google*، *Meta*، *Amazon*، *Microsoft* وغیره.
9. تدوین قوانین بین‌المللی برای عدالت دیجیتال: مشارکت فعال در نهادهای بین‌المللی برای تصویب قوانین محدودکننده سلطه سایبری قدرت‌های شمال.
10. افزایش آگاهی دهی عمومی درباره حاکمیت دیجیتال: برگزاری کارزارهای اطلاع رسانی برای افزایش سواد دیجیتال و حساسیت جامعه نسبت به موضوعات حریم خصوصی و امنیت اطلاعات.

نتیجه گیری

در پایان این تحقیق با عنوان «امنیت سایبری و استعمار دیجیتال: بررسی وابستگی زیرساخت‌های سایبری کشورهای جنوب به قدرت‌های شمال»، به نتایج مهمی دست می یابیم که نشان دهنده چالش‌های عمیق و ضرورت اقدامات راهبردی در این حوزه است.

1. تسلط ساختاری شرکت‌های فناوری شمال بر زیرساخت‌های دیجیتال جنوب: شرکت‌های بزرگ فناوری از کشورهای شمال، به خصوص ایالات متحده، با در اختیار داشتن مالکیت نرم افزارها، سخت افزارها و شبکه های ارتباطی، کنترل گسترده ای بر زیرساخت‌های دیجیتال کشورهای جنوب اعمال میکنند. این تسلط ساختاری منجر به وابستگی فنی و اقتصادی کشورهای جنوب شده و امکان بهره برداری از اطلاعات و منابع این کشورها را برای شرکت‌های شمال فراهم میسازد.
2. ظهور استعمار دیجیتال و سرمایه داری نظارتی: با گسترش فناوری‌های دیجیتال، شکل جدیدی از استعمار، موسوم به استعمار دیجیتال، بوجود آمده است. در این مدل، شرکت‌های فناوری از طریق جمع آوری و تحلیل داده های کاربران در کشورهای جنوب، نه تنها منافع اقتصادی کسب میکنند، بلکه رفتارها و تصمیم گیری‌های اجتماعی و سیاسی را نیز تحت تأثیر قرار میدهند. این فرآیند، که به سرمایه داری نظارتی معروف است، حریم خصوصی و استقلال کشورهای جنوب را تهدید میکند.
3. نقش نهادهای بین‌المللی در تقویت نابرابری‌های دیجیتال: نهادهای جهانی و مقررات بین‌المللی که بیشتر توسط کشورهای پیشرفته (شمال) ساخته شده اند، ناخواسته باعث افزایش نابرابری‌های دیجیتال شده اند. این کشورها قوانین و معیارهایی را به نفع خود تعیین کرده اند و کشورهای جنوب مجبور اند از این قوانین پیروی کنند، در حالیکه در ساختن این قوانین نقش مهمی نداشته اند.
4. ضرورت توسعه زیرساخت‌ها و سیاست‌های بومی در کشورهای جنوب: برای مقابله با چالش های در زمینه وابستگی زیرساخت های کشور های جنوب به قدرت های شمال، کشورهای جنوب باید به توسعه زیرساخت‌های دیجیتال بومی، تدوین سیاست‌های ملی در حوزه امنیت سایبری و حفاظت از اطلاعات، و تقویت توانمندی‌های فنی و انسانی خود بپردازند. همچنین، همکاری‌های منطقه و بین‌المللی با هدف تبادل دانش و تجربه میتواند به کاهش وابستگی به کشورهای شمال کمک کند.
5. تدوین چارچوب‌های جهانی برای حکمرانی عادلانه دیجیتال: در سطح جهانی، نیاز به تدوین چارچوب‌ها و قوانین بین‌المللی برای حکمرانی عادلانه دیجیتال احساس میشود. این چارچوب‌ها باید با مشارکت فعال کشورهای جنوب تدوین شده و به گونه طراحی شوند که منافع همه کشورها را در نظر بگیرند و از سلطه یک جانبه کشورهای شمال جلوگیری کنند.
6. افزایش آگاهی دهی عامه: کشور های جنوب باید از طریق برنامه های آگاهی دهی مردم خویش را از انواع مختلف سوء استفاده جوئی های فضای سایبر آگاه نموده تا این آگاهی در کاهش قربانی واقع شدن افراد در فضای سایبر کمک به عمل آورد.

در مجموع، مقابله با استعمار دیجیتال و تضمین امنیت سایبری کشورهای جنوب نیازمند تلاش‌های هماهنگ در سطوح ملی، منطقه ای و بین‌المللی است. تنها از طریق توسعه ظرفیت‌های بومی، تدوین سیاست‌های مستقل و مشارکت فعال در

حکمرانی جهانی دیجیتال میتوان به استقلال دیجیتال دست یافت و از منافع تخنیک های معاصر به صورت عادلانه مستفید شد.

منابع و مأخذ

1. اسکندری، مصطفی، 1389، شناخت استعمار، نشر قم، قم، ایران.
2. انوشا سهیل، نیکجو مهنوش و کولیوند روح اله، 1400، استراتیژی امنیت سایبری، سومین همایش ملی تحقیقات میان رشته ای در علوم مهندسی و مدیریت، محل برگزاری: تهران.
3. کامران دستجردی حسن و میر محمدی زهرا، 1393، فضای سایبری و تعاریف در جغرافیای سیاسی، فصلنامه – پژوهشی و بین المللی انجمن جغرافیای ایران، دور جدید، سال دوازدهم، شماره 43.
4. حسین سید محمد و هاشمی غازی، 1398، حقوق جزای اختصاصی 3، نشر بنیاد آسیا، کابل، افغانستان.
5. خلیلی پور رکن آبادی، و نورعلی وند یاسر، 1391، تهدیدات سایبری و تأثیر آن بر امنیت ملی، فصلنامه مطالعات راهبردی، سال پانزدهم، شماره دوم.
6. ساعی احمد، 1392، جهانی شدن و جنوب، چهارم، نشر قومس، تهران، ایران.
7. صادقی تاج محمد، رئیسی لیلا و انصاری مهیاری علی رضا، 1403، کارکرد های سازمان های منطقه ای در جنگ های سایبری، فصلنامه دست آورد های نوین در حقوق عمومی، سال سوم، شماره نهم.
8. فرشا سعید پرویز، جلالی محمود و گودرزی مهناز، 1401، ضرورت همکاری دولت ها در تقویت امنیت سایبری، فصلنامه مطالعات بین المللی، سال 19، شماره 2.
9. کتانجی الناز و پور قهرمانی بابک، 1400، چالش های امنیت سایبری در کشور های «آسه آن»، فصلنامه مطالعات بین المللی سال 18، شماره1.
10. کلانتری صمد و خلیلی عبدالرسول، 1389، جهانی شدن و روابط شمال و جنوب، فصلنامه تحقیقات سیاسی و بین المللی، شماره 3.
11. مخمل باف سیده زهره و آزاد شیرزداد، 1401، مقایسه سیاست های امنیت سایبری رؤسای جمهور آمریکا«2000-2020»، نشریه علمی مطالعات راهبردی آمریکا، سال دوم، شماره هشتم.
12. ملکوتی رسول و خلیل زاده مونا، 1400، راهکار حقوقی تأمین امنیت سایبری، فصلنامه علمی وسایل ارتباط جمعی – رسانه، سال سی و سوم، شماره 1.
13. یادگاری وحید، یسیلیانی ناصر و متین فر احمد رضا، 1396، نقش امنیت فاوا در جنگ سایبری علیه سازمان های امنیتی با رویکرد پدافند غیرعامل، فصلنامه پژوهش های حفاظتی-امنتی دانشگاه جامع امام حسین(ع)، سال ششم، شماره 1.
14. *Danielle Coleman*،2019 ، *Digital Colonialism: The 21st Century Scramble for Africa through the Extraction and Control of User Data and the Limitations of Data Protection Laws.*

15. *Longreads longreads.tni.org/digital-colonialism-the-evolution-of-us-empire? utm_source=chatgpt.com.*
16. *Reuters. "China accuses US of launching 'advanced' cyberattacks, names alleged NSA agents." April 15, 2025.*
17. *European Commission. "General Data Protection Regulation (GDPR).*
18. *Time. "Here's The Evidence Russia Hacked The Democratic National Committee." December 14, 2016.*
19. *Wikipedia. "Facebook–Cambridge Analytica data scandal.*
20. *Wikipedia. "Fancy Bear.*
21. *https://www.npr.org/2020/02/12/805498673/russian-interference-in-2016-us-election-what-you-need-to-know?utm_source=chatgpt.com.*
22. *The National Security Agency's (NSA) Surveillance Programs.*