

سب

عصر
فضای
مجازی

گزارش شماره ۵۲
فروردین ۱۴۰۰



مرکز ملی فضای مجازی
پروژه شبکه فضای مجازی

قدرت و حاکمیت سایبری

محتوای انتشار یافته در این گزارش
الزاماً بیانگر دیدگاه مرکز ملی فضای مجازی نیست

تهیه شده در معاونت فناوری
مرکز ملی فضای مجازی

تهیه کننده: نازیلا تقوایی

حقوق مادی و معنوی این اثر متعلق به مرکز ملی فضای
مجازی است و استفاده از آن با ذکر منبع مجاز می باشد.

نشانی: تهران، میدان آرژانتین، خیابان بیهقی، نبش

خیابان ۱۶ غربی، پلاک ۲۰

تلفن: ۰۲۱-۸۶۱۵۱۰۶۱

کد پستی: ۱۵۱۵۶۷۴۳۱۱

فهرست

سخن نخست ۵

مقدمه ۹

بخش اول (تعاریف قدرت)

۱-۱- دیدگاه های قدرت در تعریف قدرت ۲۲

۱-۲- قدرت ملی ۲۶

۱-۳- امنیت ملی ۲۷

بخش دوم (نظریه های روابط بین الملل)

۲-۱- قدرت سایبری ۳۷

۲-۲- رابطه قدرت سایبری و امنیت ملی در فضای سایبری ۳۸

بخش سوم (حکمرانی)

۳-۱- حاکمیت سایبری ۴۳

۳-۲- حاکمیت داده ۵۲

بخش چهارم (فضای سایبر)

۴-۱- آناتومی فضای سایبری ۵۹

۴-۲- ابعاد، مولفه ها و ویژگی های قدرت در فضای سایبری ۶۰

۴-۳- چارچوب فضای سایبری (دیدگاه David Clark) ۷۰

۴-۴- چارچوب فضای سایبری (دیدگاه Sheldon) ۷۱

بخش پنجم (مدل بلوغ امنیت سایبری)

۵-۱- مسئولیت ها و نسبت ها در فضای سایبری ۷۹

۵-۲- حاکمیت و برابری در فضای سایبری ۸۱

۵-۳- راهبردهای افزایش کارآمدی حاکمیت توسط فناوری اطلاعات و ارتباطات ۸۴

بخش ششم (فضاهای جغرافیای اعمال قدرت نرم)

۶-۱- مدل پیشنهادی برای تطبیق و سنجش قدرت نرم در فضای سایبری ۸۸

۶-۲- تحلیل مدل پیشنهادی ۹۰

۶-۳- شاخص های پیشنهادی برای سنجش قدرت سایبری بر اساس مدل پیشنهادی ۹۳

جمع بندی ۹۷

منابع ۱۰۰

فهرست جداول، نمودارها و عکس‌ها

- شکل ۱-۱ چرخه عمر قدرت ۲۰
- شکل ۱-۲ رویکردهای کلی در تعریف قدرت ۲۲
- جدول ۱-۲ نظریه‌های روابط بین الملل ۳۷
- شکل ۱-۲ مدل مفهومی ارتباط قدرت سایبری و قدرت ملی بر اساس رویکرد فرکتالی ۴۰
- شکل ۱-۳ قلمرو قدرت در فضای مجازی ۴۵
- شکل ۱-۴ ابعاد، مولفه‌ها و ویژگیهای قدرت در فضای سایبر ۶۲
- شکل ۲-۴ چارچوب فضای سایبر از دیدگاه David Clark- 2010 ۷۱
- شکل ۳-۴ چارچوب فضای سایبری از دیدگاه Sheldon - 20119 ۷۱
- جدول ۱-۵ خلاصه‌ای از مدل‌های بلوغ قدرت سایبری ۷۸
- شکل ۱-۵ الگوی مفهومی مناقشات در عصر اطلاعات ۸۰
- شکل ۱-۶ لایه‌های افقی فضای سایبری ۸۸
- شکل ۲-۶ مدل پیشنهادی برای تبیین قدرت نرم در فضای سایبر ۹۰
- جدول ۱-۶ تحلیلی از گزاره‌های قدرت در مدل پیشنهادی ۹۴

سخن نخست



فضای مجازی با شتاب شگرف و رو به تزایدی که در حال بسط و گسترش است تمام ساحات اجتماعی، اقتصادی، سیاسی و فرهنگی زندگی بشر را درنوردیده و هر روز بخش بزرگی از زندگی واقعی را در خود فرو برده و حیات متفاوت و جدیدی به آن می‌دهد. لذا به نظر می‌رسد دو نگاه کلان به فضای مجازی وجود دارد: نگاه اول که بالاخص در ابتدای رشد و تکوین فضای مجازی مسلط شده بود، آن را همچون ابزاری کنار سایر ابزارهای بشری تصویر می‌کرد که تنها طریقت داشت. اما نگاه دوم، در نتیجه رشد تحولات خیره‌کننده فضای مجازی و سایه گسترش آن در حوزه‌ها و شئون بشر در یک دهه اخیر آن را چون سکویی می‌داند که بسیار فراتر از شأن ابزاری حیات انسان‌ها را سامان جدیدی داده و ادعای تمدن نوینی را دارد. رویکردی که از قضا از چشمان بصیر رهبر انقلاب نیز دور نمانده و انتظاری تمدنی از فضای مجازی در ایران را مطالبه داشته‌اند.

در همین راستا گزارش‌های عصر فضای مجازی تلاش می‌کند تا فهم سازمان‌ها و دستگاه‌های مرتبط با حوزه فضای مجازی را ارتقاء بخشیده و آن‌ها را برای مواجهه فعال و خردمندانه با تحولات این عرصه مهیا سازد.

سید ابوالحسن فیروزآبادی
دیرشورای عالی و رئیس مرکز ملی فضای مجازی

مقدمه



فضا و قدرت سایبری اصطلاحات رایجی هستند، اما تعریف و اندازه گیری آن ها بسیار دشوار است. ویژگی های منحصر به فرد فضای سایبر می تواند برای تحقق قدرت نرم استفاده شود که هدف اصلی آن تغییر رفتار افراد و شکل دهی به ترجیحات آن ها از طریق جذب یا اقناع به جای زور است (نای، ۲۰۱۰). در مفهوم سنتی قدرت، قدرت سخت مطرح است که به دنبال تغییر رفتار با تهدید و اجبار مستقیم است. به موازات پیشرفت تکنولوژی، رویکرد قدرت نرم به عنوان جایگزین و یا همراه روش های قدرت سخت نظامی به وجود آمد. قدرت نرم، عوامل انسانی را هدف قرار می دهد و هدف آن ترغیب دیگران برای درخواست خروجی های مطلوب از طریق مفاهیمی مانند فرهنگ، ارزش های سیاسی و سیاست خارجی است (ترورتن و جونز، ۲۰۰۰). مزایای قدرت نرم به عنوان سیاست جذابیت آفرینی در مقابل زور، می تواند به عنوان یک ابزار جایگزین برای دستیابی به اهداف ملی به شمار آید.

1. Policy, Economy, Social, Technology, Environment and Law

احتمالی حمله با تحلیل نقاط قوت و ضعف جامعه هدف^۱، برای کاهش نفوذ و توانایی آنها برای عملکرد آزادانه در فضای مجازی ارائه داده و حملات را از دیدگاه جوامع هدف ارزیابی نموده و شرایطی را برای مدافعان حکومت و کشور فراهم می‌کند که مخاطرات در فضاهای مختلف را شناسایی و در جهت مقابله با آن اقدام نمایند. در مفهوم سنتی قدرت، قدرت سخت مطرح است که به دنبال تغییر رفتار با تهدید و اجبار مستقیم است (Nye، ۲۰۱۰). به موازات پیشرفت تکنولوژی، رویکرد قدرت نرم به عنوان جایگزین و یا همراه روش‌های قدرت سخت نظامی به وجود آمد. قدرت نرم عوامل انسانی را هدف قرار می‌دهد و هدف آن ترغیب دیگران برای درخواست خروجی‌های مطلوب از طریق مفاهیمی مانند فرهنگ، ارزش‌های سیاسی و سیاست خارجی است^۲ (Treverton and Jones، ۲۰۰۰). مزایای قدرت نرم به عنوان سیاست جذابیت‌آفرینی در مقابل زور، می‌تواند به عنوان یک ابزار جایگزین برای دستیابی به اهداف ملی به شمار رود. ظهور فضای مجازی و مفهوم قدرت سایبر، باعث ضرورت یافتن ارزیابی چگونگی تحقق قدرت و نفوذ در یک جهان بهم پیوسته شده است. از آنجا که فضای مجازی فاقد مرزهای فیزیکی و در عین حال نابالغ^۳ است، ملتها قدرتی برای حفظ مرزها و یا راه‌هایی برای تهدید مرزهای همسایه با استفاده از تعاریف متداول قدرت را ندارند و عدم بلوغ در این فضا، به مرور زمان منجر به ناپایداری و تضعیف قدرت در آن می‌گردد. مدل پیشنهادی، با در نظر گرفتن لایه‌های

1.Target society

2.«get others to want the outcomes that you want»

3.Unmatured

با در نظر گرفتن لایه‌های فضای سایبر در تقاطع با ابعاد جغرافیای
اعمال حاکمیت و شاخص‌های PESTEL، امکان تحلیل، تطبیق و
سنجش قدرت سایبر را فراهم می‌کند و همچنین می‌تواند راهکاری
برای رسیدن به مدل بلوغ^۱ برای فضای سایبر و سنجش قدرت برای
آن باشد.

بخش اول

تعاریف قدرت



بخش اول

تعاریف قدرت

قدرت در تعریف عام اشاره به توانایی اثر گذاری بر رفتار دیگران یا جریان وقایع دارد. اما تعاریف علمی و دقیق از این مفهوم به شدت پراکنده و متنوع‌اند. قدرت در کلی ترین حالت خود اغلب به عنوان مترادف با حکومت قلمداد می شود. قدرت در مفاهیم روانشناسی و به عنوان یک ویژگی در قلمروهای نظامی، اقتصادی، سازمانی و سیاسی، همواره مرتبط با مفهوم نفوذ، تحمیل و کنترل قلمداد می شود. قدرت در تمامی حوزه های علوم قابل بسط و معنی دار است.

چرخه عمر قدرت در شکل ۱ نشان داده شده است. با توجه به شکل، برای مثال منبع تولید قدرت، متغیری وابسته به حداقل دو عامل بستر تولید قدرت و فرآیند تولید قدرت است. قدرت از بستری جهت تولید، فرآیند تولید، منابع تولیدکننده، فرآیند توزیع و نحوه به کارگیری (اعمال) و اثر به کارگیری برخوردار است. این مراحل، شکل دهنده چرخه عمر قدرت می باشند. به منظور درک

ماهوی قدرت، شناخت هر یک از گام های چرخه عمر قدرت ضروری به نظر می رسد.

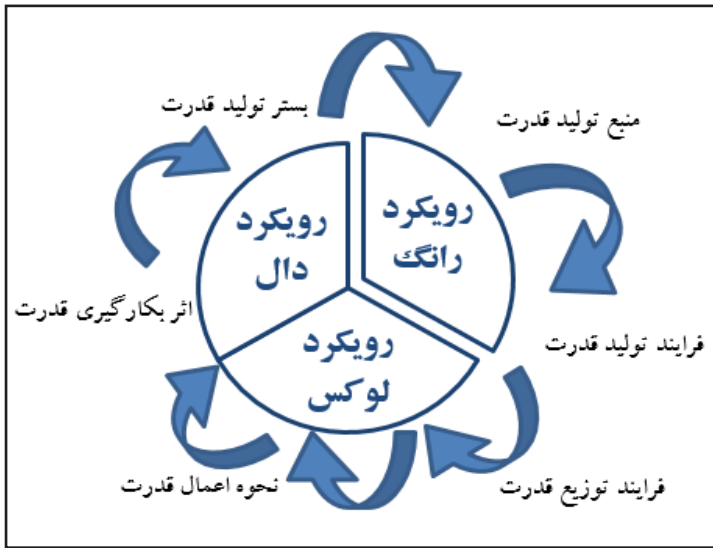
قدرت پژوهان کلاسیک، در این که کدام مرحله را مفهوم واقعی قدرت تلقی نمایند، دچار تردید و اختلاف نظر می باشند. گروهی چون دال بر این باورند که زمانی می توان از قدرت صحبت به میان آورد که شاهد کاربرد آن باشیم. گروهی دیگر چون رانگ قدرت را بر مبنای توانش، قابلیت یا داشته، تعریف می کنند و قدرت را بر اساس منابع تولیدکننده و فرآیند تولید، تفسیر می کنند. گروهی دیگر از جمله لوکس، قدرت را در کالبد ساختار و از نگاه اعمال کننده آن در نظر گرفته اند.

بر اساس چرخه عمر قدرت، سه رویکرد اصلی در تعریف قدرت وجود دارد. رویکرد اول هابز-لوکس، قدرت را از منظر عاملیت بررسی کرده اند. مفهومی خارج از اختیار فرد و متعلق به روابط میان ساختارها. چنین قدرتی مادی و عینی است که ریشه در نقش ها، قواعد، مراجعات، موقعیت ها و روابط ساختاری دارد. رویکرد دوم، راسل و وبر، قدرت را از منظر خروجی بررسی نموده و نتیجه و اثر را ملاک اصلی در تعیین قدرت می داند. از منظر وبر، مفاهیم قدرت و سلطه یکسان اند و به قدرت از نوع قدرت سخت و زور نگاه می کند. دنیس رانگ، اثر و نیت را منشأ قدرت می داند. رویکرد سوم، قدرت را از منظر چگونگی تولید قدرت بررسی می نماید. به اعتقاد این گروه، قدرت ظرفیت و استعداد است. همان طور که پیشتر بیان گردید، پارسونز قدرت را در

کالبد نظامات اجتماعی قرار داده است. جریان های اجتماعی در نگاه پارسونز در مسیر تولید، به کار بستن و توزیع قدرت حائز اهمیت است. گیدنز ظهور این ظرفیت در هر عامل انسانی را امکان پذیر دانسته است.

برداشت کامل قدرت از نگاه گیدنز، ظرفیت و استعدادی است که در مقام عمل موجب تغییر گشته و بازیگر می تواند نتایج حاصله را پاس دارد. از دیدگاه فوکو، سه چهره قدرت مطرح است: قدرت گفتمانی که بر منابع (زمین، تولیدات و داشته ها) اعمال می گردد، قدرت دیسیپلینی، سازمانی یا انضباطی که جلوه در رفتار دارد و بر طبیعت جسمانی نفوذ می کند و سرانجام قدرت مشرف بر حیات. از نظر هابز، مفهوم قدرت با مرجعیت حکومت مطرح است. او معتقد است به طور طبیعی در جوامع انسانی بی قانونی مطرح است. اما با ظهور حکومت، مردم، قدرت متفرق در نیت خود را به حاکمیت تفویض نموده و قدرت از شرایط طبیعی به شرایط مدنی ارتقا می یابد. بنابراین مرجع قدرت هابزی در حکومت است و اقتدار حکومت ناشی از کسب قدرت است.

بدین ترتیب قدرت، توان ایجاد تغییر و توان تولید اثر دلخواه برای هر یک از بازیگران تعریف می شود. این اثر می تواند در حوزه های گوناگون سیاسی، اجتماعی، فرهنگی، اقتصادی و اطلاعاتی ظهور یابد. از منظر لوکس منابع تولید کننده، فرآیند توزیع و نحوه به کارگیری (عاملیت) قدرت، محورهای کلیدی در شناخت قدرت می باشند.



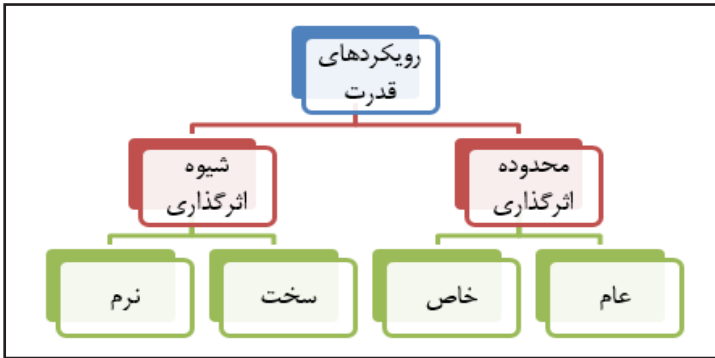
شکل ۱-۱- چرخه عمر قدرت

قدرت یک دولت، توانایی او برای انجام امور خود یا وادار ساختن دیگران برای انجام آن است؛ این قدرت برگرفته از قدرت نفوذ این دولت یا رهبری آن بر جهان یا قدرت نظامی یا اقتصادی با نفوذ مالی یا امکانات دیگر آن است. قدرت، پدیده‌ای متغیر و به شدت پویا بوده و از ساختاری عمیق و چندلایه برخوردار است. دگرگونی در هر یک از لایه‌های قدرت، سبب تغییر در ماهیت لایه و در نهایت معنای عام قدرت خواهد شد. جنس قدرت در نگاه سنتی منفی است و به عنوان یک پدیده در اختیار و متعلق به طبقه حاکم (دولت) است و مفاهیمی چون سلطه و نفوذ، ذهنیت به شدت غیرعادلانه‌ای

را از قدرت ایجاد می کند. نگاه دیگر به قدرت، مشارکتی و توزیع شده است؛ جلوگیری از تمرکز آن و شکل دهی قدرت دسته جمعی، دوطرفه و چند طرفه است. در این نگاه، قدرت پدیده ای مثبت است. رویکرد های مختلفی در تعریف قدرت مطرح است. از دیدگاه شیوه اثر گذاری، قدرت را می توان در دو گروه سخت و نرم تعریف نمود.

قدرت سخت به دنبال تغییر رفتار با تهدید و اجبار مستقیم از طریق روش های سخت نظامی است. در حالی که قدرت نرم، توانایی تغییر رفتار و شکل دهی به ترجیحات دیگران از طریق جذابیت آفرینی یا اقناع به جای زور است.

از دیدگاه محدوده اثرگذاری، قدرت به دو گروه عام^۱ و خاص^۲ قابل تعریف است. قدرت های عام درصدد افزایش محدوده جغرافیایی سلطه خود، جهت تبیین و اعمال قدرت هستند. به موازات پیشرفت تکنولوژی، قدرت ها دریافته اند که دیگر قدرت عام، اهداف آن ها را برآورده نمی کند. بنابراین به مجموعه ای از نهادهای کوچک و فراملیتی با محدوده اثرگذاری خاص که تضمین کننده قدرت آن ها در فضای نرم است، روی آوردند.



شکل ۱-۲- رویکردهای کلی در تعریف قدرت

۱-۱- دیدگاه های مختلف در تعریف قدرت

در یک نگاه کلی، قدرت به معنی استفاده از منابع مادی و معنوی به منظور اعمال اراده و تأثیرگذاری بر دیگران و ایجاد رفتار مطلوب توسط آنهاست. به طوری که در فقدان آن، طرف مقابل مجبور، متمایل یا مشتاق به اطاعت نباشد. در تقسیم بندی انواع قدرت، دیدگاه های مختلفی وجود دارد. نبوی در کتاب فلسفه قدرت، آن را به سه دسته الهی، ماشینی و انسانی تقسیم کرده است. در این دیدگاه، ابعاد اقتصادی، نظامی، سیاسی، دینی و فرهنگی زیرمجموعه قدرت انسانی است.

در مکتب اسلام، قدرت اصلی از آن خداست و تمامی قدرت ها در طول قدرت الهی و در پرتو مشیت او قرار می گیرد. قدرت، امانتی در اختیار انسان برای هدایت جامعه در مسیر تحقق اهداف برپایی عدالت و تأمین مصالح اجتماعی و کسب کمالات اخلاقی است و هدف غایی نیست.

ریموند دووال و مایکل بارنت^۱ (۲۰۰۵) در کتاب «قدرت و سیاست در عرصه بین الملل» انواع قدرت را به چهار دسته اجباری (استفاده از منابع مادی و هنجاری یک بازیگر برای تحت تأثیر قرار دادن وضعیت و کنش‌های بازیگر دیگر)، ساختاری (توانایی تأثیرگذاری بر نتایج با استفاده فناوری و روابط ساختاری)، نهادی (کنترل بازیگر دیگر از طریق قواعد و رویه‌های خاص اجتماعی و نهادهای رسمی و غیررسمی) و مولد (تولید گفتمان، سوژه‌ها و معانی خاص برای جهت دهی روابط بین عوامل قدرت در جامعه) تقسیم بندی کرده اند.

جوزف نای، قدرت را به سه دسته نرم (کسب نتیجه مطلوب از طریق جاذبه و بدون استفاده از اجبار یا تطمیع)، سخت (توانایی تغییر رفتار دیگران از طریق اجبار یا تطمیع) و هوشمند (توانایی ترکیب قدرت نرم و قدرت سخت) تقسیم کرده‌اند. وی قدرت نرم را توانایی شکل‌دهی به ترجیحات دیگران از طریق جذب یا اقناع به جای زور تعریف می‌کند (نای، ۲۰۱۱).

از منظر لوکس، منابع تولید کننده، فرآیند توزیع و نحوه به‌کارگیری (عاملیت) قدرت، محورهای کلیدی در شناخت قدرت می‌باشند. او قدرت را در کالبد ساختار و از نگاه اعمال کننده آن در نظر می‌گیرد. بر اساس مفهوم هژمونی از دیدگاه گرامشی، قدرت این‌گونه تعریف می‌شود که گروه دارای قدرت، ارزش‌های اجتماعی را به گونه‌ای تغییر می‌دهد که دیگران با رضایت از آن‌ها تبعیت کنند. در تعریف قدرت به مثابه توانمندی سیستم اجتماعی، رویکرد کارکردگرایی ساختی

1. Barnett & Duvall

پارسونز-مرتون مطرح است. بر اساس این دیدگاه، قدرت ویژگی سیستم برای رشد و بقاست بطوریکه نهادهای اجتماعی دارای کارکردهایی در جهت افزایش انسجام، انطباق، دستیابی به اهداف و حفظ ارزش‌های جامعه^۱ (AGIL) باشند. قدرت به عنوان عامل تغییر رفتار و اعمال سلطه، توانمندی سیستم اجتماعی و جایگاه آن در نظام جهانی است. الگوی AGIL یکی از چارچوب‌های تحلیل محتوایی ارزش‌های فرهنگی و روش نسبتاً ساده‌ای برای تشریح تفاوت‌های فرهنگی سازمان‌ها است. پارسونز در الگوی خود، هر یک از چهار بعد فرهنگ سازمانی را با یکی از حروف کلمه AGIL معرفی می‌نماید. در واقع طبق این الگو، هر سیستم اجتماعی باید چهار وظیفه را در جهت بقا و پیشرفت انجام دهد که عبارت‌اند از:

انطباق^۲: برای انطباق، یک سیستم اجتماعی باید از محیط و چگونگی تغییرات آن به خوبی آگاه باشد و متناسب با آن خود را تعدیل و تنظیم کند.

دستیابی به هدف^۳: به این معنی که سیستم اجتماعی باید دارای فرایندی باشد که اهداف موردنظر و نیز راه‌های دستیابی به آن‌ها را مشخص نماید.

انسجام و یکپارچگی^۴: به این معنی که تمام سیستم‌های اجتماعی نیاز دارند که اجزای آن‌ها از گسیختگی و ازهم‌پاشیدگی حفظ شود. قسمت‌های مختلف یک سیستم باید با یکدیگر در ارتباط بوده، وابستگی متقابل آن‌ها درک شده و با هم هماهنگ باشند.

-
1. Adaptation Goal Integration Latent pattern maintenance
 2. Adaptation
 3. Goal Attainment
 4. Integration

نهفتگی^۱: نهفتگی مشتمل بر دو مسئله مرتبط است: کنترل تنش‌ها (تنش‌ها و فشارهای درونی کنشگران) و حفظ الگوها (نشان دادن رفتار «مناسب»). سیستم‌های اجتماعی باید برای آنکه انگیزه کافی را در کنشگران، برای ایفای نقش‌شان (الگوی حفظ)، ایجاد کنند، راه‌هایی بیابند و همچنین باید سازوکارها و سوپاپ‌های اطمینانی برای کنشگران فراهم آورند که آنان بتوانند ناکامی‌ها و سایر فشارهای روحی انباشته‌شده‌شان را آزاد سازند.

در دیدگاه‌های قدرت به مثابه جایگاه در نظام جهانی، دیدگاه والرش‌تاین مطرح است که در آن یک بازیگر سیاسی-اقتصادی موقعیت مرکزی‌تری در نظم سرمایه‌داری داشته باشد. بر این اساس، این بازیگر از یکی از موقعیت‌های زیر برخوردار است:

ژئوپلیتیک: قدرت بازیگران سیاسی برای ایجاد انحصار چندگانه (الیگوپولی) در حوزه حاکمیت خود و تدوین قواعد و هنجارهای نظام بین‌الملل و تحمیل آن بر بازیگران ضعیف‌تر

ژئواکونومیک: قدرت بازیگران اقتصادی در کسب موقعیت مرکزی‌تر در نظام تقسیم‌کار جهانی به منظور انباشت بیشتر سرمایه و جذب ارزش‌افزوده از پیرامون به مرکز نظام

ژئوکالچر: قدرت ایدئولوژی و ارزش‌های فرهنگی جوامع با فرهنگ بنیادین نظام جهانی سرمایه‌داری برای انباشت سود بیشتر

قدرت درون سیستمی: قدرت اقتصادی-سیاسی-فرهنگی برای احراز موقعیت مرکزی در نظام جهانی سرمایه‌داری نظیر قدرت آمریکا و چین

1. Latent pattern maintenance

قدرت بیرون سیستمی: قدرت اقتصادی-سیاسی-فرهنگی برای چالش کشیدن نظام جهانی سرمایه‌داری نظیر قدرت انقلاب اسلامی

۲-۱- قدرت ملی

در یک تعریف کلی، قدرت ملی شامل مجموعه‌ای از توانایی‌ها و ظرفیت‌های کشور به منظور حفظ ارزش‌ها و منافع ملی یک کشور است. منابع قدرت ملی به منابع ثابت (منابعی که از اراده رهبران سیاسی و گروه‌های اجتماعی خارج است مانند جغرافیای سیاسی، منابع طبیعی، فرهنگ سیاسی، روحیه ملی) و منابع متغیر (فرایند حاکم بر نظام بین‌الملل و برداشت و اراده نخبگان سیاسی حاکم، مانند فناوری‌های پیشرفته، تنظیم روابط خارجی، جذب یا طرد اندیشه‌ها) تقسیم می‌شود.

تعامل و همسویی مؤلفه‌های تشکیل‌دهنده قدرت، با مبانی ارزشی و آرمان‌های یک کشور، موجب هم‌افزایی و هم‌گرایی قدرت ملی خواهد شد. به همین نسبت اتکای این مؤلفه‌ها بر ارزش‌ها و هنجارهای وارداتی، ضعف و واگرایی آن‌ها را در بر خواهد داشت. با این حال، کشورها برای حفظ موجودیت خود و نقش‌آفرینی مؤثر در عرصه جهانی ناگزیر از انعطاف‌پذیری لازم برای تطبیق خود با محیط بین‌الملل در مقاطع زمانی مختلف هستند. در این راستا، مفاهیم دیگری همچون اقتدار، نفوذ و هژمونی نیز مطرح است:

اقتدار^۱: به معنای قدرت مشروع و مقبول نظام حاکم بر یک کشور است.

نفوذ^۲: به معنای تسلط و حاکمیت پنهانی و وادار نمودن طرف مقابل به انجام عملی برخلاف میل و حتی بدون اطلاع وی است. **هژمونی**: به معنای تلاش برای دستیابی به سلطه ایدئولوژیک و فرهنگی بدون استفاده از زور و اجبار و با جلب توجه و متقاعد کردن طرف مقابل به رهبری اعمال کننده قدرت در زمینه های فرهنگی و اجتماعی است.

۳-۱-۱- امنیت ملی

امنیت ملی، وضعیت و شرایطی است که یک کشور، در بعد عینی علی‌رغم وجود تهدید، خود را قادر به حفظ منافع و ارزش های اساسی بداند و در بعد ذهنی نیز از هجوم (فیزیکی و غیرفیزیکی) به بنیان های ملی خود، هراسی نداشته باشد. امنیت ملی به عنوان یکی از مشتقات امنیت در مرزهای جغرافیایی یک کشور به صورت امنیت داخلی (مصونیت بنیان های ایدئولوژیک مکتب حاکم و حفظ حاکمیت) و امنیت عمومی (حفظ حقوق و مصالح افراد، گروه ها و نهادی اجتماعی) تعریف شده است. امنیت ملی، معادل فقدان تهدید عینی و ذهنی علیه بنیان های حیاتی و مشروعیتی یک ساختار سیاسی و ایجاد بستر مناسب حیات، ترقی، رفاه یا حتی نفوذ است.

-
1. Authority
 2. Penetration

بخش دوم

نظریه های روابط بین الملل



بخش دوم

نظریه های روابط بین الملل

از آغاز ایجاد رشته روابط بین الملل، دو نظریه خردگرایی و تامل گرایی در روابط بین الملل مطرح بوده است.

نظریه خردگرایی: بر این باور است که هویت و منافع کنشگران پیش از تعامل اجتماعی شکل می گیرند و افراد صرفاً به دلایل راهبردی روابط اجتماعی خواهند داشت. این نظریه ساختارگرا بوده و بر همین اساس، روابط بین الملل را در قالب دولت‌ها تصویرسازی می‌کند. در این نظریه مبنای تمایز کنشگران حاکمیت است، دولت‌ها به‌عنوان تنها کنشگران جهانی شناخته می‌شوند و متافیزیک روابط بین الملل نیز در قالب نظام متشکل از دولت‌های ملی دارای حاکمیت تعریف می‌گردد. از این‌رو، مفاهیم «امنیت ملی» و «منافع ملی» به‌عنوان مفاهیم اسطوره‌ای شناخته شده و در ساختار نظام بین الملل شکل می‌گیرند. در نظریه خردگرایی، قدرت مفهوم تک‌بعدی داشته و تأثیر تکنولوژی نیز بر قدرت محدود بود و تنها نقش ابزاری داشت.

نظریه تأمل گرایی: پس از جنگ جهانی دوم و در طی جنگ سرد، روابط بین‌الملل از توجه صرف به امور مادی گذر کرده و تمرکز خود را بر امور معنایی و اجتماعی نهاد. این تغییر تمرکز، موجب خلق نظریه تأمل گرایی در روابط بین‌الملل شده است. نظریه تأمل گرایی بر معناگرایی استوار است و توجه ویژه‌ای به مسائل جامعه‌شناختی و اقتضائات زمانی در تفسیر رفتار کنشگران دارد. این نظریه بر مبنای پساساختارگرایی ارائه شده است و منفعت را در چارچوب جوامع تعریف و تفسیر می‌نماید. به عبارت دیگر، در این نظریه کنشگران ذاتاً اجتماعی هستند و امکان تعریف هویت‌های متکثر برای بازیگران یکسان وجود دارد. تأمل‌گرایان معتقدند که ادعا درباره حقیقت را نمی‌توان مورد قضاوت درست یا نادرست بودن (آن‌چنان‌که نظریات مبنای معتقدند) قرار داد. زیرا مرجع بی‌طرفی برای این مسأله موجود نمی‌باشد (غیر اثبات‌گرایانه هستند).

متناسب با این تحول نظری، مفهوم قدرت ملی نیز تغییر یافته و ابعاد جدیدی را در بر گرفته است. در دوره‌ای که روابط بین‌الملل بر مبنای خردگرایی تعریف می‌شد (از ۱۹۱۹ تا ۱۹۸۰)، قدرت در دو نوع ابزاری و ساختاری تبیین می‌گردید.

قدرت ابزاری، قدرتی است که رفتار انسان را با انحصار بر جهان مادی و از طریق نیروی فیزیکی شکل می‌داد. در حالی که منظور از قدرت ساختاری، قدرتی است که رفتار انسان را از طریق قواعد و نهادها و با انحصار و کنترل جهان اجتماعی شکل می‌دهد. در این دوره مؤلفه‌هایی

همچون گستردگی جغرافیایی، تعداد جمعیت و حجم منابع طبیعی به عنوان عناصر اصلی برتری قدرت میان دولت‌ها سنجیده می‌شده است. تأسیس نهادهای بین‌المللی نیز بر مبنای نگاه ساختارگرایانه به قدرت و در راستای تقویت قدرت ساختاری کشورهای استعمارگر بوده است.

پس از پایان جنگ سرد و هم‌زمان با افزایش قدرت‌های نظامی و اقتصادی کشورها، کاربری فناوری اطلاعات نیز به سرعت فراگیر شده و اینترنت به عنوان یک خدمت جهانی، مناسبات اجتماعی را تحت تأثیر قرار داد. تکنولوژی‌های جدید باعث افزایش (یا کاهش) توانایی کنشگران سابق (دولت‌ها) شده و کنشگران جدیدی را در سطح جهان به وجود آوردند. توسعه فضای مجازی و فراتکنولوژی‌ها از یک سو موجب تقویت جامعه جهانی، اهمیت افکار عمومی و در نتیجه کاهش مطلوبیت قدرت سخت و کاربرد نیروی نظامی شده و از سوی دیگر، موجب تغییر هویت بازیگران بین‌المللی، افزایش ظرفیت تعامل و اقتدار شهروندان و بازیگران غیردولتی، غیرسرزمینی شدن فضای سیاسی و در نتیجه تمرکززدایی از قدرت شده است. در این عصر، قدرت ملی صرفاً بر مبنای ویژگی‌های سرزمینی و عوامل مادی تعریف نمی‌شود و ابعاد، دامنه و مکانیسم‌های اعمال قدرت در عرصه بین‌الملل متنوع‌تر و پیچیده‌تر شده است.

این فناوری‌ها، فرصت تغییر هویت و درک بازیگران اجتماعی از خود را برای دیگر بازیگران فراهم نمودند و بر همین اساس تعریف جدیدی

از قدرت در جوامع علمی ارائه شد. در تعریف جدید، قدرت رابطه‌ای به‌عنوان نوعی علیت توضیح داده می‌شود که در آن رفتار بازیگر موجب تغییر در رفتار بازیگر می‌شود و رفتار نیز شامل باورها، دیدگاه‌ها، عقاید، انتظارات و آنچه زمینه کنش است، تعبیر می‌شود. بر همین اساس وزارت دفاع آمریکا، فضای سایبر را به عنوان پنجمین حوزه جنگاوری^۱ بعد از زمین، دریا، هوا و فضا می‌داند.

از مجموع این مطالب می‌توان نتیجه گرفت که شرح و تفسیر روابط بین‌الملل در عصر فضای مجازی و شکل اثرگذاری فضای سایبر و فراتکنولوژی‌ها بر سیاست بین‌الملل، با استفاده از نظریه تامل‌گرایی کارآمدتر است و امکان نگاشت چهار مفهوم اصلی روابط بین‌الملل (شامل حاکمیت^۲، قدرت، جنگ و دیپلماسی) بر فضای سایبر راحت‌تر صورت می‌پذیرد.

۱) حاکمیت: در فضای فیزیکی به «امکان اعمال اراده بر یک سرزمین مشخص بدون دخالت عوامل خارجی» تعبیر می‌گردد. لذا نگاشت این مفهوم در فضای سایبر به «انحصار صلاحیت و عدم دخالت خارجی در فضای سایبری» قابل تفسیر است. مطابق با این نگاشت اگر مرز جغرافیایی به‌عنوان «حوزه یا محدوده‌ای که هر حکومت امکان اعمال حکمرانی و حاکمیت داشته باشد» در نظر گرفته شود، آنگاه جغرافیای سایبر به سه محدوده (۱) فضای نزدیک (حوزه یا محدوده‌ای از فضای مجازی که مستقیماً توسط دولت‌ها کنترل و حفاظت می‌شود)، (۲) فضای میانه (حوزه یا محدوده‌ای از فضای مجازی که

1. warfare
2. Sovereignty

توسط شرکت‌ها یا دولت دیگر کشورها اداره می‌شود ولی امکان کنترل و حفاظت بر روی آن طبق قرارداد مشخصی وجود دارد) و (۳ فضای دور (حوزه یا محدوده ای از فضای مجازی که هیچ‌گونه کنترل محلی بر روی آن وجود ندارد) قابل تقسیم است.

(۲) **قدرت:** به «توانایی اثرگذاری بر رفتار دیگران» تفسیر می‌شود و قدرت در فضای سایبر، به مسائلی چون نحوه اعمال قدرت در فضای سایبری تأکید دارد. قدرت سایبری با دو عامل خاستگاه قدرت و نحوه ایجاد یا اعمال قدرت به سه گروه اصلی پیشنهاد می‌گردد:

• «قدرت سخت-نرم»؛ به معنای استفاده از ابزارهای اطلاعاتی

در بسترهای نظامی و یا تجاری؛

• «قدرت نرم- سخت»؛ تولید قدرت سخت در فضای سایبر

توسط منابع سایبری (مانند بات نت ها، بدافزارها و اجبار مادی و فیزیکی بر افراد و شرکت‌ها در بستر فضای سایبری)؛

• «قدرت نرم- نرم»؛ گردش اطلاعات سایبری در فضای سایبر

برای جذب شهروندان کشورهای دیگر (تبلیغات سیاسی در فضای مجازی) با هدف تأثیرگذاری بر دیدگاه‌های افراد که در آن‌هم ابزار و نحوه اعمال قدرت، نرم است و هم خاستگاه قدرت؛

(۳) **جنگ:** در جامعه جهانی به مجموعه عملیات و اقدامات قهرآمیز مسلحانه‌ای گفته‌ای می‌شود که در چارچوب مناسبات کشورها (اعم از دو یا چند کشور) روی می‌دهد و موجب اجرای عواید خاصی در

کل مناسبات آن‌ها با یکدیگر و همچنین کشورهای ثالث می‌شود. با این تعریف و با توجه به انواع قدرت سایبری که در بخش قبل ارائه شد، مفهوم جنگ در فضای سایبری به انواع سخت و نرم آن قابل تعمیم است. منظور از جنگ سخت در فضای سایبری، استفاده از زیرساخت‌ها و خدمات زیربنایی فضای سایبر برای ضربه زدن به دیگر کشورها است. جنگ نرم نیز درباره بهره‌گیری از ظرفیت‌های فضای سایبر (انواع محتوا و خدمات محتوایی) برای تأثیرگذاری بر افکار عمومی کشورها قابل تفسیر است.

۴) دیپلماسی: به مدیریت روابط خارجی با سایر دولت‌ها و سایر کنشگران روابط بین‌الملل و مشارکت در تصمیم‌گیری و اجرای سیاست خارجی گفته می‌شود. دولت‌ها می‌توانند با استفاده انجام مذاکرات، تبادل نمایندگی‌ها، توسعه همکاری‌ها و دیدارها و گفتگوها به اهداف و منافع خود دست یابند. آن‌چنان‌که پیش‌ازاین شرح داده شد، در دیدگاه خردگرایی دولتی‌ها به‌عنوان تنها کنشگران روابط بین‌الملل شناخته می‌شدند، اما در دیدگاه تامل‌گرایی کنشگران جدیدی پا به عرصه روابط بین‌الملل گذاشته‌اند. در دیدگاه تامل‌گرایی، جامعه مدنی و بخش خصوصی (علاوه بر دولت‌ها) به‌عنوان بازیگران جدید و اثرگذار در روابط بین‌الملل نقش‌آفرینی می‌کنند و تا حد قابل توجهی بار دیپلماسی دولت‌ها را به دوش می‌کشند. این نهادهای نوظهور غیردولتی از طریق ایجاد اتحادهای فراملیتی، همکاری‌های بین‌المللی یا حتی طرح دعای فرامرزی، هم

دامنه اثرگذاری دولت‌ها را بسط داده‌اند و هم میزان تأثیرگذاری بر دیگر دولت‌ها را افزایش داده‌اند. علاوه بر این، ضمن کاهش هزینه در تأثیرگذاری بر دیگر کشورها، هزینه مقاومت کشورهای رقیب را نیز به شدت افزایش می‌دهند.

تامل گرایی	خردگرایی	
۱۹۸۰ به بعد	۱۹۱۹ - ۱۹۸۰	دوره طرح
چند هویتی	تک هویتی	ویژگی کنشگران
در روابط اجتماعی شکل می‌گیرد.	پیش از شروع رابطه تعیین می‌شود	ویژگی منافع
جامعه	حاکمیت	مبنای تمایز کنشگران
دولت، بخش خصوصی و جامعه مدنی	دولت‌ها	کنشگران اصلی
امور معنایی و جامعه شناختی	ساختارها و امور مادی	نقطه تمرکز
پست مدرنیسم و پسا استعمارگرایی	نئو نالیسم و نئولبرالیسم	مکتب مرتبط

جدول ۱-۲- نظریه های روابط بین الملل

۱-۲- قدرت سایبری

قدرت سایبری، توانایی به کارگیری منابع، ظرفیت‌ها و قابلیت‌های مبتنی بر فضای سایبر به منظور پشتیبانی از قدرت ملی و دستیابی به اهداف راهبردی در فضای سایبر و خارج از آن است. از دیدگاه دانیل کوهل، قدرت سایبری به معنای توانایی استفاده از فضای سایبر برای ایجاد برتری و تأثیرگذاری روی محیط‌های عملیاتی دیگر است.

زیمت و باری، قدرت سایبری را قابلیت کنترل سامانه‌های فناوری اطلاعات و شبکه‌های فضای سایبر می‌دانند که برای انجام مأموریت‌های نظامی و پشتیبانی از حوزه‌های اقتصادی و سیاسی قابل استفاده است.

جووزف نای، قدرت سایبری را قدرت مبتنی بر منابع اطلاعاتی فناوری‌های ارتباطی می‌داند.

از دیدگاه شلدون، قدرت سایبری توانایی دستیابی به اهداف راهبردی و کاهش توانایی دشمن در بهره‌برداری یا حمله به زیرساخت‌های فضای سایبر است. وی قدرت سایبری را یک ابزار مکمل برای قدرت ملی می‌داند که می‌تواند برای استفاده توسط دولت مردان یک کشور جذاب باشد.

از نظر اسپید، قدرت سایبری توانایی یک دولت-ملت برای برقراری، کنترل و اعمال نفوذ در داخل و از طریق فضای سایبر برای پشتیبانی و پیوستگی با دیگر عناصر حوزه قدرت ملی است. در این تعریف دستیابی به قدرت سایبری به توانایی دولت برای توسعه منابع جهت عملیات در فضای سایبر متکی است.

۲-۲- رابطه قدرت سایبری و امنیت ملی در فضای سایبری

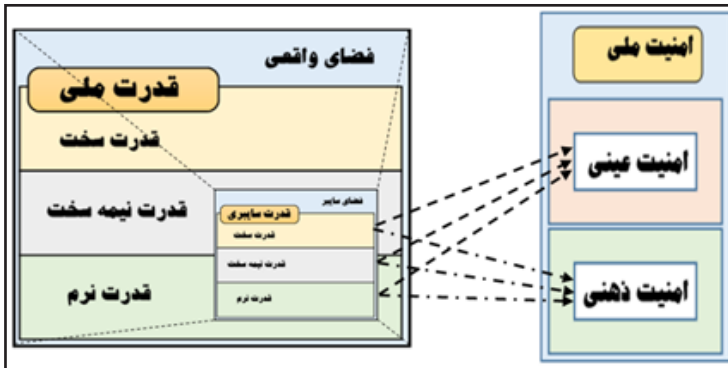
قدرت سایبری رابطه‌ای انکارناپذیر با امنیت ملی دارد چراکه فضای سایبر نوع جدیدی از تهدیدات، متفاوت با تهدیدات سنتی علیه امنیت ملی را به وجود آورده است. برخی از این تهدیدات مانند جرائم سایبری، جاسوسی سایبری، تروریسم سایبری و جنگ سایبری منافع ملی کشورها را برای دستیابی به اهداف سیاسی و ایدئولوژیکی با چالش‌های جدی روبرو ساخته است. علاوه بر آن، امنیت ملی در فضای سایبر با چالش‌های نوینی مانند صیانت از ارزش‌ها، هنجارها

و هویت ملی، تلاش برای مشروع نشان دادن نظام سیاسی حاکم، تأمین امنیت مبادلات مالی و احقاق حقوق مادی و معنوی و اعمال قوانین در فضای سایبر مواجهه است.

بر مبنای نظریه دانیل کوهل، رویکرد فرکتالی برای قدرت سایبری انتخاب شده است. در این رویکرد، قدرت سایبری یک فرکتال از قدرت ملی محسوب می‌شود. چون دارای تمامی ویژگی‌های قدرت ملی در فضای سایبر است و تمامی منابع و فرآیندهای قدرت ملی در قدرت سایبری نیز وجود دارد. امروزه دولت‌ها قدرت ملی خود را با قدرت سایبری پیوند زده‌اند و از آن به‌عنوان کاتالیزور و شتاب‌دهنده قدرت استفاده می‌کنند. علاوه بر آن، توانایی دولت‌ها برای مهار چالش‌های امنیت ملی در فضای سایبر از مهم‌ترین عوامل قدرت سایبری دولت‌ها محسوب می‌شود.

رویکردی که در آن، عملکرد یک پدیده جزئی، به صورت نگاشتی از یک پدیده کلان با ویژگی‌های مشابه بررسی می‌شود، رویکرد فرکتالی شناخته می‌شود. فرکتال از واژه لاتین فرکتوس^۱ به معنی شکسته شدن به قطعات نامنظم گرفته شده است. بسیاری از پدیده‌های طبیعی که در ظاهر بی‌نظم به نظر می‌رسند از یک تکرار منظم در مقیاس‌های متفاوت برخوردارند. یکی از ویژگی‌های پدیده‌های فرکتالی، خود متشابه بودن آن‌ها است. اگر یک تصویر فرکتال را به چند بخش تقسیم کنیم، هر بخش یک نسخه از کل تصویر را نمایش می‌دهد و با آن مشابه است. ویژگی دیگر فرکتال‌ها، تشکیل از راه تکرار است.

1. fractus



شکل ۲-۱- مدل مفهومی ارتباط قدرت سایبری و قدرت ملی بر اساس رویکرد فرکتالی

ویژگی فرکتالی قدرت ملی موجب می‌شود تا فرآیندها و پدیده‌های آن، با یک نگاشت در قالب قدرت سایبری بررسی شوند. پارادایم فرکتالی، یک پارادایم کل‌نگر است که هر کدام از اجزا می‌تواند بر روی کل اثر بگذارد. امنیت ملی در فضای سایبر نیز همانند فضای واقعی شامل دو مؤلفه امنیت عینی (فقدان تهدید) و امنیت ذهنی (فقدان ترس و نگرانی) در نظر گرفته می‌شود.

بخش سوم

حکمرانے



بخش سوم حکمرانه

حکمرانی سیستم پیچیده‌ای از تعاملات بین ساختارها، سنت‌ها، مسئولیت‌ها و عملکردها به وسیله سه ارزش کلیدی پاسخگویی، شفافیت و مشارکت و در واقع روش پیاده‌سازی قدرت یا چگونگی اعمال قدرت است.

۱-۳- حاکمیت سایبری

حاکمیت به این معنی است که یک کشور بتواند بدون وابستگی، تمام تصمیمات مربوط به خود را گرفته و تنها محدود به قوانین بین‌المللی و قدرت نسبی خود در جهان باشد. حاکمیت، بنا به تعریف فرهنگ علوم سیاسی سیادت قانونی ملت و دولت ملی، درون قلمرویی معین، با اتکا به قوای درون (و بدون تکیه به قوای بیرون از مرزهای قلمروی مربوط) است. حاکمیت، از سوی دولت و برای تحکیم قدرت دولت اعمال می‌شود، اما در اصل، منبعث از وحدت و اجماع شهروندان است. طبق تعریف لوکس، قدرت در رژیم و حاکمیت ریشه دارد. در این رویکرد ساختارها به عنوان نظامات

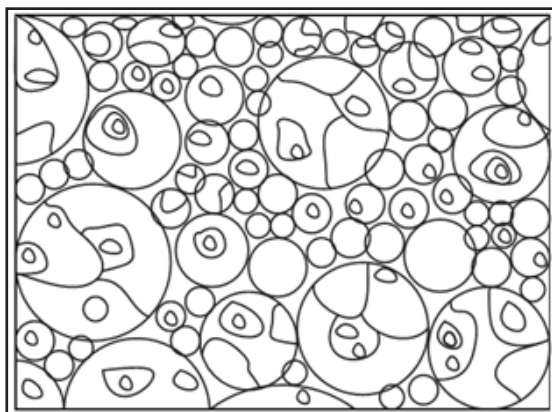
1. Sovereignty

مشروع تلقی می شوند که قدرت در آن‌ها متمرکز گردیده است [۱۱] مفهوم حاکمیت در فضای مجازی بسیار پیچیده است. سناریوهای مختلف و نامحدودی می توان در تئوری برای آن در نظر گرفت. دو سناریو ممکن برای حاکمیت در فضای مجازی وجود دارد [۱۰].

در سناریوی اول، دولت به طور مستقل بر فضای سایبری که در قلمروهای حاکم بر آن‌ها قرار دارد، بر پایه زیرساخت‌های فیزیکی در داخل مرزهای خودکنترل دارد. یا اینکه دولت، تصمیم می گیرد که هیچ‌گونه کنترلی اعمال نکرده و اساساً مالکیت فضای سایبری خود را به سایر ملل و نهادهای غیردولتی مجاز واگذار می کند. در سناریوی اول، فضای سایبر، درست مانند دنیای واقعی امروز است. بازیگران غیردولتی تحت کنترل دولت عمل می کنند.

در سناریوی دوم، قدرت های سایبری در همه انواع می تواند شکل گیرد. هر نهاد، از جمله یک بازیگر غیردولتی، به طور بالقوه می تواند یک دولت اینترنتی باشد. در فضای مجازی یک نهاد می تواند با اختیار خود و حقوق مستقل، فعالیت ها را کنترل کند. فضای مجازی محیط های سیاسی، اجتماعی و اقتصادی متنوعی را شامل می شود که هر کدام در یک سلسله مراتب قدرت بسیار پویا با یکدیگر تعامل می کنند. ممکن است اشخاص به طور مداوم با هدف نفوذ، دستیابی به منابع و رسیدن به قدرت، سوءاستفاده‌هایی انجام دهند. بعضی حوزه ها صلح‌آمیز خواهند بود و برخی دیگر مملو از اختلاف است. بعضی از آزادی کامل برخوردارند و برخی، محدودیت‌های

شدید را متحمل می شوند. در شکل ۱-۴- فضای سایبری به صورت حباب های ریز نشان داده شده که در آن حوزه های مختلف با هنجارها و مرزهای نامعلوم و نامشخص وجود دارد. در این سناریو، فضای سایبر موجب از بین رفتن قدرت های بزرگ و شکل گیری قدرت های کوچک تر و همچنین بازیگران غیردولتی خواهد شد.



شکل ۳-۱- قلمرو قدرت در فضای مجازی

حاکمیت خود در قانون بین الملل یک مفهوم واضح است. در حالی که حاکمیت سایبری به طور کلی مفهوم مبهمی است که اغلب در ارتباط با قدرت دولتی و استقلال در فضای مجازی استفاده می شود. بنابراین، مفهوم حاکمیت سایبری باید دقیق تر تعریف شود.

مفهوم حاکمیت به صلح وستفالن^۱ در سال ۱۶۴۸ بازمی گردد که بر اساس آن، دولت ها باید بر سرزمین های خود و امور داخلی، حاکمیت داشته تا دیگر دولت ها نتوانند در امور آنها دخالت کنند (فرانزس^۲، ۲۰۰۹). اصل حاکمیت که از حقوق بین الملل

1. Westphalian
2. Franzese

جدا نیست، با اصل برابری هم مرتبط است. بدان معنا که همه دولت‌ها تحت قانون بین‌المللی با هم برابرند. بنابراین هیچ دولتی بر دولت دیگر برتری ندارد (جنسن^۱، ۲۰۱۵). علاوه بر این، حاکمیت یکی از عناصری است که دولت را تحت قانون بین‌المللی تعریف می‌کند. بر این اساس، یک دولت به عنوان یک موجودیت مستقل، باید دارای جمعیت، قلمرو، قدرت سیاسی و حاکمیت باشد (دیلیر^۲ و همکاران، ۲۰۰۹).

اصل حاکمیت، مستلزم حقوق و تعهدات است. حقوق در دو سطح تعیین می‌شود: داخلی و بین‌المللی. حقوق داخلی از این واقعیت ناشی می‌شود که دولت‌ها می‌توانند در سرزمین خود اقدام کنند. آن‌ها در فعالیت‌های داخلی خود مستقل هستند. در سطح بین‌المللی، این حق شامل توانایی‌های دولت‌ها برای نمایندگی از سرزمین و مردم خود در انجمن‌های بین‌المللی است. در سطح بین‌المللی، حاکمیت دولت باید با اصول حقوق بین‌الملل، از جمله تصمیمات شورای امنیت سازمان ملل متحد و قانون جنگ‌های مسلحانه مطابقت داشته باشد. وظایف مربوط به حاکمیت شامل تعهد در به رسمیت شناختن حاکمیت کشورهای دیگر، عدم دخالت در امور آن‌ها و کنترل اقدامات بازیگران در قلمرو دولت خود است.

بالین‌حال، ماهیت عدم وجود مرزهای مشخص در فضای مجازی، حاکمیت دولت را تحت‌الشعاع قرار می‌دهد و این سؤال مطرح می‌شود که آیا اصول حقوق بین‌الملل می‌تواند به فضای مجازی

1. Jensen

2. Daillier

اعمال شود یا خیر؟ تولید فناوری و فضای سایبر، مفاهیم سنتی در تعریف مرزهای دولت و اصول قانون بین المللی را به چالش می کشد. در روزهای اول ظهور این فناوری، اینترنت به عنوان ابزاری برای حکمرانی نام برده می شد و این باور وجود داشت که در نتیجه آن آزادی بیان به وجود می آید. بهر حال شواهد نشان می دهد که حضور دولت در توسعه فضای سایبر در نهایت اجتنابناپذیر است. هنگامی که مشخص شد فناوری می تواند برای اهداف سیاسی استفاده شود، حکمرانی به عنوان اصل اساسی دولت نمی تواند به سادگی نادیده گرفته شود. برخی بازیگران اقتصادی، برای حفظ کسب و کار و سایر بخش های اقتصادی در فضای سایبری، تقاضای حکمرانی بیشتری در این فضا داشتند. این درخواست ها نشان می دهد که مفهوم حکمرانی همچنان به درستی تفهیم نشده یا مفهوم آن در قانون بین المللی تحریف شده است. توسعه فضای مجازی و فناوری به طور قابل توجهی دنیای مدرن را تغییر داده و موجب ارزیابی دوباره اصول سنتی حقوق بین الملل مانند حاکمیت شده است. در روزهای اولیه این فناوری، اینترنت توسط کاربران آن اداره می شد و اعتقاد بر این بود که به دلیل وابستگی به متولیان آن و ماهیت فراملیتی خود، تحت حاکمیت دولت عمل نخواهد کرد. باین حال، با افزایش تعداد کاربران اینترنت در سرتاسر جهان و استفاده های بالقوه از آن در حوزه های نظامی و سیاسی، مشخص شد

که ایالات متحده به طور فزاینده‌ای نفوذ خود را برای در دست گرفتن، حداقل درجه‌ای از حاکمیت در فضای مجازی نشان می‌دهد. پس از آن، نقش حاکمیت دولتی در فضای مجازی به طور گسترده در ادبیات علمی مورد بحث قرار گرفت. گروه کارشناسان دولتی سازمان ملل متحد^۱ (UNGGE) تصمیم گرفت که حقوق بین‌الملل، از جمله حاکمیت دولت، در فضای مجازی مورد استفاده قرار گیرد (مجمع عمومی سازمان ملل متحد، ۲۰۱۵). این تصمیم به این معنی است که قانون معارضه^۲ در فضای مجازی و همچنین تمام حقوق و تعهدات مرتبط با اصول حاکمیت، قابل اجرا است. راهنمای تالین مربوط به حقوق بین‌الملل و جنگ سایبری و کتاب راهنمای تالین^۳ ویرایش ۲۰۰ که در مورد وضعیت حقوق بین‌الملل کنونی در زمینه فضای سایبری بحث می‌کند، به نتیجه‌گیری مشابهی در مورد حاکمیت دولت در فضای مجازی رسیده است. این آثار به چگونگی استفاده از اصول حقوق بین‌الملل در فضای مجازی و چالش‌های منبعث از آن می‌پردازند (جنسن، ۲۰۱۵، ۲۰۱۱). این کتاب، حاکمیت در فضای مجازی و نیز کنترل برخی از دولت‌ها بر محتوای اینترنت و توجیه قانونی برای سانسور بر پایه اصول حاکمیت دولتی را تحلیل می‌کند.

واقعیتی که در اکثر آثار دانشگاهی بر مفاهیم حقوقی حاکمیت در فضای مجازی وجود دارد، نشان می‌دهد که مسئله حاکمیت سایبری، اغلب به عنوان یک ماده از قانون بین‌المللی مطرح می‌شود. اگرچه

حاکمیت سایبری در آثار علمی مرتبط به طور کامل مورد بحث و بررسی قرار گرفته است، اما پیوستگی لازم در این تعاریف وجود ندارد و هنوز ابهاماتی در آن دیده می‌شود. تعاریف مندرج در این آثار، از مفهوم سنتی حقوق بین‌الملل نسبت به فضای سایبری تا مفاهیم گسترده‌ای از کنترل و استقلال متغیر است. این رویکرد نسبت به تعریف حاکمیت سایبری - از لحاظ نظارت و استقلال دولتی در فضای مجازی - یک بحث جنجالی است، زیرا ممکن است تفکیک مسائل مربوط به استقلال راهبردی از مفهوم حاکمیت سایبری را در نظر نگیرد. در حالی که خودمختاری به حاکمیت دولت بسیار مرتبط است، باین حال خودمختاری و استقلال راهبردی با مفهوم حاکمیت مترادف نیستند. پس از تحلیل روند به‌کارگیری مفهوم حاکمیت سایبری، مشخص شد که بعضی از فعالان اقتصادی و دولتی، نگرانی‌های بیشتری در مورد تأثیرات مالی کنترل داده دارند. برای رفع این شکاف، بحث حاکمیت داده به تجزیه و تحلیل روند جامع حاکمیت سایبری افزوده شد. هدف این بحث تکمیلی، تعریف صریح حاکمیت داده بوده و به تجزیه و تحلیل استفاده از این اصطلاح برای درک بهتر آن می‌پردازد. در ادامه تعاریف مختلفی از اصطلاح حاکمیت داده مورد بررسی قرار می‌گیرد.

تحقیقات در استفاده از مفاهیم حکمرانی و حکمرانی سایبری در راهبرد های ملی امنیت سایبری نشان می‌دهد که تعداد کمی از دولت‌ها از واژه حکمرانی استفاده می‌کنند و واژه حکمرانی سایبری تنها توسط

دولت کانادا استفاده می‌شود. این مفهوم در ابتدا توسط دولت های غربی بکار رفت که به تعریفی از حکمرانی اشاره دارد که کاملاً با قانون بین‌المللی همخوانی دارد.

راهبرد های امنیت سایبری در بیشتر کشورها نشان می دهد که حملات سایبری ممکن است تهدیدی برای حاکمیت دولت باشد و تأکید آن‌ها بر حفاظت از حاکمیت دولت است. برای رسیدن به این هدف، دولت ها برای بهبود امنیت سایبری در فن آوری های اطلاعاتی و شبکه های دولتی، دفاع و زیرساخت های حیاتی برنامه ریزی هایی انجام داده‌اند. بحث غالب محققان این حوزه، حقوق و تعهدات مرتبط با حاکمیت دولت و نحوه استفاده از آن در فضای مجازی و همچنین بعد فیزیکی حاکمیت در فضای مجازی است. زیرساخت های فیزیکی برای عملکرد مناسب فضای مجازی ضروری است و اکثر این زیرساخت ها در قلمرویی قرار دارند. بنابراین حاکمیت دولتی در فضای مجازی می تواند به عنوان توسعه‌ای از حاکمیت ارضی دولت در نظر گرفته شود.

هنجارهای حاکمیت قبلی در فضاهای طبیعی (غیرسایبری) شکل گرفت و به عنوان یک عامل جهانی شناخته شد. درحالی‌که مقایسه توسعه هنجارهای حاکمیت در سایر حوزه ها نشان داد که بحث درباره کاربرد حاکمیت در شرایط جدید، طی یک دوره زمانی قابل توجهی، تکامل یافته است. فضای مجازی که ساخته دست انسان است، ممکن است به عنوان یک عامل جهانی در نظر گرفته

نشود و تعریف مشابهی در جهان نداشته باشد.

به طور کلی، بحث های مربوط به حاکمیت در حوزه های دیگر شبیه به موضوعات مربوط به فضای مجازی بود و نشان داد که مسائل حاکمیت در فضای مجازی یک شبه حل نخواهد شد. در نهایت، این تحلیل روند نشان می دهد که رایج ترین درک از حاکمیت سایبری، از تعریف آن از حقوق بین الملل مشتق شده است. همچنین ورود بخش اقتصاد اروپا و مقامات فرانسوی به این حوزه به بحث های جایگزین در مورد حاکمیت سایبری منجر شد که بر استقلال راهبردی حاکمیت سنتی تأکید دارد.^۱ مفهوم استقلال راهبردی به حفاظت گسترده تر از حاکمیت دولتی نیاز دارد و دولت هایی را شامل می شود که بر روی پردازش داده ها، ذخیره سازی داده ها و زیرساخت های فناوری اطلاعات کنترل دارند. بنابراین، لازم است تفاوت بین استقلال راهبردی و حاکمیت دولت در نظر گرفته شود.

اظهارات ادوارد اسنودن در مورد برنامه نظارت بر انبوه اینترنت آژانس امنیت ملی آمریکا (NSA^۲) در سال ۲۰۱۳ نشان داد که سلطه کشورها در حوزه فناوری اطلاعات و ارتباطات آسیب پذیر است. آسیب پذیری ها در هر دو وجه سخت افزار و نرم افزار، صرفاً آسیب پذیری های فنی نیستند، بلکه مربوط به دسترسی دولت ها به اطلاعات مربوط به جمعیت دیگری نیز می باشد. آگاهی های اسنودن، باعث سلب اعتماد از این فناوری ها و فعالیت های اینترنتی در آمریکا شد. کارهای اسنودن موجی از خشم در میان دولت ها برانگیخت و انعکاس آن

۱. درک فرانسوی از حاکمیت از لحاظ استقلال استراتژیک از فرهنگ استراتژیک فرانسه حاصل می شود که به دنبال دستیابی به این نوع خودمختاری است و دولت را به عنوان نیرو محرکه توسعه استقلال استراتژیک در سطح اتحادیه اروپا به حساب می آورد.

2. National Security Agency

منجر به ایجاد روندهایی برای محافظت از آنچه که حاکمیت سایبری نامیده می‌شود، گردید. به دلیل نقض حاکمیت دولت توسط چنین نفوذهایی و کمپین‌های جاسوسی گسترده، لازم است میان استقلال راهبردی مربوط به امنیت سایبری و حاکمیت سایبری که طبق قوانین بین‌المللی تعریف شده است، تمایز قائل شویم. علاوه بر این، نگرانی سابق در مورد ناتوانی دولت در تمامی سطوح بزرگ راهبردی، برای ادغام منابع نظامی، اقتصادی، دیپلماتیک و اطلاعاتی با قابلیت‌های سایبری بر اساس فن‌آوری‌های قابل اعتماد همچنان وجود دارد.

۲-۳- حاکمیت داده

در این بخش مفهوم حاکمیت داده به طور دقیق تجزیه و تحلیل شده است که پیشتر در اولین تحلیل از تحول حاکمیت نادیده گرفته شده بود. مفهوم حاکمیت داده فاقد تعریف مشخص و ثابت است، اما به طور مرتب در سیاست و صنایع مورد استفاده قرار می‌گیرد. حاکمیت داده به عنوان توانایی دولت برای کنترل داده‌های ایجاد شده در برابر عبور آن از قلمرو خود تعریف می‌شود. تحقیقات نشان می‌دهد که این اصطلاح در راهبرد های ملی مورد استفاده قرار نگرفته است، اما ممکن است در سطوح سیاسی دیگر مورد بحث قرار گیرد. پس از افشای ادوارد اسنودن درباره نظارت بر انبوه رسانه‌های ایالات متحده در ماه ژوئن ۲۰۱۳، بسیاری از دولت‌ها شروع به پیاده‌سازی راهکارهای فنی و حقوقی برای کنترل اطلاعات

منتقل شده از سرزمین‌های خود کردند. در ابتدا، تلاش‌ها بر حفظ داده در یک قلمرو خاص و عدم عبور آن از مرزها متمرکز شد. راه‌حل‌های فنی پیشنهادی شامل: ایجاد کانال ارتباطی زیردریایی برای اینترنت بین آمریکای لاتین و اروپا از طریق کابل، ساخت یک شبکه مسیریابی منطقه‌ای ایجاد سرویس محاسباتی ابری ملی و استفاده از سرویس ایمیل ملی بود. ناکارآمدی و بی‌ثمر بودن این راهکارهای فنی در جلوگیری از نظارت و نفوذ خارجی در مورد داده‌ها ثابت شده است. کارشناسان فنی معتقدند که با رمزگذاری بهتر داده‌ها می‌توان از داده‌های مربوط به یک منطقه خاص محافظت نمود. ایده حاکمیت می‌تواند در سال ۱۶۴۸ به صلح وستفالن برسد. یک حکومت مستقل، بر سرزمین فیزیکی و امور داخلی خود قدرت و حاکمیت دارد. به عبارت دیگر، دولت‌ها حق دارند که خود را همان‌گونه که مناسب می‌دانند، کنترل کنند و سایر دولت‌ها باید موقعیت آن‌ها را محترم شمرده و در امور داخلی آن‌ها دخالت نکنند. در جهان مدرن، اصل حاکمیت بسیار مهم است. اصل حاکمیت با پایه‌ریزی قانون و نظم بین‌المللی شکل می‌گیرد. پس از آن اکثر راهکارهای حاکمیت داده بر محاسبات ابری و استانداردگذاری پلتفرم‌های مبتنی بر اینترنت متمرکز شدند. اظهارات ادوارد اسنودن ترس بین‌المللی را افزایش داد و منجر به سرمایه‌گذاری فزاینده دولت‌ها بر حفاظت از اطلاعات و عبور از سرزمین‌های خود شد.

حاکمیت داده یک مفهوم قانونی و مشخص نیست و دامنه وسیعی از تعاریف را شامل می‌شود. پترسون و همکارانش در سال ۲۰۱۱ حاکمیت داده را به عنوان راهی برای محدود کردن انتقال و ذخیره داده‌ها به یک قلمرو خاص تعریف کردند. این تعریف فاقد مفهوم کنترل است و قصد کنترل اطلاعات در آن مشاهده نمی‌شود. دی فیلیپ^۱ و مکاری^۲ (۲۰۱۲)، حاکمیت داده را به عنوان امکان کنترل کاربران بر روی داده‌های خود تعریف می‌کنند، اما این تعریف نیز فاقد عنصر کنترل دولتی بر روی داده‌ها است. بر اساس تعریف پولیشن ربن^۳ و رایت^۴ (۲۰۱۴) حاکمیت داده، اراده یک دولت برای کنترل اطلاعات تولید شده یا عبور آن از قلمرو خود است و شامل مجموعه‌ای از اقدامات برای دستیابی به این کنترل است. این پژوهشگران حاکمیت داده را زیرمجموعه حاکمیت سایبری در نظر می‌گیرند.

1. De Filippi
2. McCarthy
3. Polatin-Reuben
4. Wright

بخش چهارم

فضای سایبری



بخش چهارم

فضای سایبر

در سال ۲۰۱۰، ایالات متحده به طور رسمی فضای سایبری را به عنوان حوزه پنجم قدرت به رسمیت شناخت و با ایجاد واحد فرماندهی سایبری ایالات متحده، فرماندهی یکپارچه آن از نیروهای مسلح به فرماندهی راهبردی ایالات متحده واگذار شد. فرمان سایبری ایالات متحده مرتبط با حوزه های زمین، دریا، هوا و فضا می باشد. اگرچه فضای سایبری یک قلمرو مجازی است، اما نفوذ جهانی را می توان سریع تر و فراگیر تر از هر قلمرو دیگری در آن مورد بررسی قرار داد.

فضای سایبری برای اهداف دیپلماتیک و اطلاعاتی بسیار مؤثر است. فناوری های اینترنتی موجب اشتیاق عموم مردم به اخبار فوری شده و دولت ها را برای انجام دیپلماسی دیجیتالی تحت تأثیر قرار می دهد. دولت ها از فضای اینترنتی برای اطلاع رسانی به شهروندان در مورد سیاست های عمومی، بیان موقعیت های دیپلماتیک به صورت پویا و حتی گسترش اطلاعات غلط استفاده می کنند.

در ژوئن ۲۰۱۳، جان کری وزیر امور خارجه آمریکا تقریباً بلافاصله از طریق یک توییت به نظر وزیر خارجه بریتانیا پاسخ داد. وزارت امور خارجه ایالات متحده معتقد است سفیران این کشور باید حساب‌های تویتر داشته باشند تا بتوانند سریعاً دیپلماسی عمومی را انجام دهند. کوبا نیز که دارای روابط رسمی با ایالات متحده نیست، از فضای سایبری به عنوان یک کانال برای فعالیت های دیپلماتیک استفاده می کند. بازیگران غیردولتی نیز فضای سایبری را برای دیپلماسی و ابتکارات اطلاعاتی استفاده می کنند. القاعده برای جذب اعضای جدید از اینترنت استفاده کرده و با استفاده از آن برای ساخت دستگاه‌های تروریستی و بمب‌گذاران انتحاری ایجاد انگیزه می کند. شورن^۱ تخمین می زند که ۵۰۰۰ وب سایت تروریستی محور که جوانان را رادیکالیزه کرده اند، وجود دارد. باین حال، استفاده از فضای مجازی این امکان را به وجود آورد تا شهروندان بتوانند دیکتاتورهای قدیم مانند مبارک مصر را شکست دهد. در بیداری اسلامی، انقلابیون به‌طور مؤثر از رسانه‌های اجتماعی برای تبلیغ برنامه‌های سیاسی، افزایش آگاهی و جذب حمایت و بودجه استفاده کرده و حتی فعالیت های ده‌ها هزار معترض را در زمان واقعی هماهنگ کردند.

فضای سایبری، یک میدان جنگ جدید است که در آن بسته‌های شبکه می‌توانند تقریباً بلافاصله در سراسر جهان ارسال شوند تا سیستم های فیزیکی، از جمله دارایی‌های زیرساختی حیاتی در چهار حوزه فیزیکی و قلمرو سایبری را تحت تأثیر قرار دهند. حملات

1.Schorn

سایبری ۲۰۰۷ به استونی، وبسایت‌های دولتی^۱ و رسانه‌های این کشور را تعطیل کرد. بدافزار Stuxnet در سال ۲۰۱۰ در سانتریفیوژهای هگزا فلوراید اورانیوم را نابود کرد. از این رو همه کشورها در حال توسعه قابلیت‌های سایبری خود هستند.

از طرفی، فضای سایبری به حوزه اقتصادی مهم بدل شده است. تقریباً تمام فعالیت‌های بانکداری در این فضا رخ می‌دهد. تجارت الکترونیک در حال شکوفایی است و شرکت‌هایی مانند گوگل و آمازون نشان داده‌اند که امکان تبدیل دارایی‌های مجازی به ثروت واقعی وجود دارد و امکان ایجاد کسب‌وکارهای مختلف در محیط‌های ابری وجود دارد.

ظهور فضای مجازی و مفهوم قدرت سایبری نیاز به ارزیابی چگونگی تحقق قدرت و نفوذ در یک جهان به هم پیوسته دارد. از آنجاکه فضای مجازی فاقد مرزهای فیزیکی است، ملتها قدرتی برای حفظ مرزها و یا راه‌هایی برای تهدید مرزهای همسایه با استفاده از تعاریف متداول قدرت را ندارند.

۱-۴- آناتومی فضای سایبری

فضای مجازی، با استفاده از زیرساخت اطلاعات و ارتباطات فراگیر، محیطی غنی برای پیش‌بینی قدرت و نفوذ فراهم نموده است. همه انواع بازیگران اعم از دولت‌ها، شرکت‌ها، سازمان‌های تروریستی و جنایتکار و گروه‌های غیرانتفاعی جنبه‌های حیاتی عملیاتشان را در

۱. در این سال کشور استونی در معرض سلیلی از حملات سایبری قرار گرفت که کل زیرساخت‌های اینترنتی کشور را تحت تأثیر خود قرار دادند و البته هدف اصلی وبسایت‌های دولتی و سازمانی، بانکها و روزنامه‌ها بودند. با توجه به زمانبندی حملات که در زمان مجادله این کشور و روسیه بر سر برداشتن یادبود شوروی از پایتخت استونی بود، مقامات استونی روسها را عامل اصلی این حملات می‌دانند. با این حال مثل همیشه امکان ردیابی منشأ اصلی این نوع از حملات وجود نداشته و نخواهد داشت.

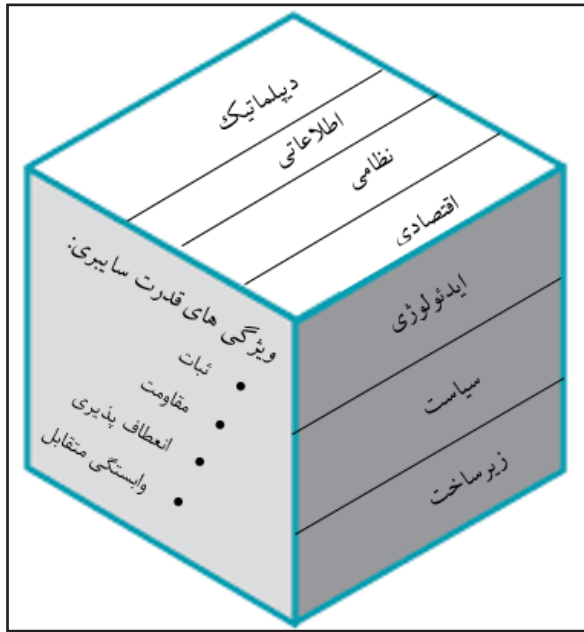
در فضای مجازی اجرایی کرده و امیدوارند که مزایای ارائه شده توسط این قلمرو را به دست آورند. فضای مجازی، یک اکوالایزر^۱ (یک ابزار هموارکننده) است و این امکان را ایجاد می‌کند که همه بازیگران، از قابلیت‌های مانند دسترسی سریع، ناشناس بودن و محافظت و توانایی ایجاد و مشارکت در اقتصادهای مجازی و استفاده از سلاح‌های سایبری را با قیمت پایین بهره‌گیری نمایند. این امر به شدت معادله قدرت را تغییر می‌دهد. شکاف بین قدرت‌های بزرگ را افزایش داده و این امکان را به بازیگران غیردولتی می‌دهد که قدرت سایبری را به دست گیرند.

۲-۴- ابعاد، مؤلفه‌ها و ویژگی‌های قدرت در فضای سایبری

قدرت سایبری دارای سه مؤلفه حیاتی است: ایدئولوژی، سیاست بدنه و زیرساخت‌های بدنه. این مؤلفه‌ها دارای چهار ویژگی هستند که بازیگران را قادر می‌سازد تا قدرت سایبری را دست گیرند: ثبات^۲، مقاومت^۳، انعطاف‌پذیری و وابستگی متقابل^۴. این چهار ویژگی در بخش‌های زیر به‌طور دقیق مورد بحث قرار می‌گیرند. چهار بعد قدرت (دیپلماتیک، اطلاعاتی، نظامی و اقتصادی) که به‌طور سنتی در رابطه با اشکال فیزیکی آن مورد بحث قرار می‌گیرند به قدرت‌های اینترنتی نیز اعمال می‌شود. هر چند تمام ابعاد قدرت دارای ارزش مختص خود هستند، قدرت اقتصادی (یا حداقل حمایت اقتصادی از قدرت دیگری) به عنوان مهم‌ترین بعد برای تداوم

1. Equalizer
2. Stability
3. Resilience
4. Interdependency

حیات یک قدرت سایبری شناخته می شود. زیرا بدون منابع مالی، یک قدرت سایبری نمی تواند ایدئولوژی خود را دنبال کرده، از نظر سیاسی کسی را جذب نموده و یا زیرساخت های لازم را ایجاد کند. بنابراین منابع مالی برای انجام فعالیت هایی که به رشد و انعطاف پذیری قدرت سایبری در ابعاد دیگر (دیپلماتیک، اطلاعاتی و نظامی) کمک می کنند، نیز مهم است. اقتصاد دنیای واقعی و اقتصاد سایبری باید به هم مرتبط باشند و دلیل آن، نیاز فضای سایبری به منابعی از دنیای واقعی برای تداوم فعالیت خود است. تعاملات قوی بین این دو اقتصاد جهت حصول اطمینان از تداوم حیات یک قدرت سایبری ضروری است. چنین تعاملاتی در مورد گوگل و اینترنت وجود دارد. گوگل محصولات و خدمات اینترنتی را ایجاد می کند و آن ها را با هدف کسب درآمد به فروش می رساند. از آن درآمد برای ایجاد پیشنهادات جدید که درآمد بیشتری دارند استفاده کرده و این چرخه ادامه می یابد. گوگل، با به کارگیری اینترنت زیرزمینی^۱، از منابع واقعی برای تقویت فعالیت هایش در فضای مجازی استفاده می کند.



شکل ۴-۱- ابعاد، مؤلفه‌ها و ویژگی‌های قدرت در فضای سایبر

• ثبات

ثبات یک نهاد سایبری در صورتی قابل قبول است که بتواند موجودیت خود را حفظ کرده و به فعالیت خود ادامه دهد. این ویژگی، چندین جنبه مربوط به مؤلفه‌های یک نهاد سایبری و چهار بعد قدرت را شامل می‌شود. بنابراین یک نهاد سایبری باید با توجه به هر یک از مؤلفه‌های قدرت سایبری و نیز تأثیر در طول چهار بعد قدرت، قابل اجرا باشد.

• ایدئولوژی، سیاست و زیرساخت

به منظور حفظ ثبات، هر سه مؤلفه قدرت سایبری - ایدئولوژی، سیاست و زیرساخت‌ها - باید حفظ شده و به طور مداوم با تغییر محیط، نوسازی شوند و ایدئولوژی به طور خاص، نباید استاتیک و ثابت بوده و باید در محدوده خود تکامل یابد. این تکامل، امکان تحقق دستورالعمل‌های گسترده، تضمین یک حرکت مثبت و ایجاد یک زیرساخت با ثبات را برای نهادها فراهم می‌کند. نمونه‌ای از این تکامل، ایدئولوژی جمهوری خلق چین است که از کمونیسم مائوئیست در طی انقلاب فرهنگی در دهه ۱۹۷۰ تا نسخه فعلی آن - لیبرالیسم اقتصادی - تکامل یافته است. به طور مشابه، بدنه سیاسی نیز باید تجدید و جوان‌سازی شود و اطمینان حاصل شود که ایدئولوژی، مأموریت و بدنه حاکم، بروز است. ساختار و وضعیت حکومت ممکن است بر اساس محیط و خواسته‌های اعضای آن تنظیم شود. جمعیت سیاسی بدنه نیز باید به گونه‌ای تحقق یابد تا ایده‌ها، رهبران و اعضای جدیدی را بپذیرد که تعهد داشته و مأموریت و دستورالعمل‌ها را ترویج می‌دهند. همانند ایدئولوژی و سیاست، زیرساخت‌های سایبری نیز باید همراه با پیشرفت‌های فناوری و شرایط سیاسی، اجتماعی و اقتصادی تغییر یابد.

1.Underground

• مقاومت

مقاومت - تداوم موجودیت یک نهاد - یکی دیگر از ویژگی‌های مهم قدرت سایبری است. میزان مقاومت نهادها در فضای مجازی، برگرفته از اهمیت آن‌ها در فضای فیزیکی است. به‌طور کلی دو جنبه برای مقاومت وجود دارد که عبارت‌اند از: الف) عمل کردن در سطح مناسب توسط نهاد دارای قدرت سایبری جهت تحقق دستور کار خود ب) حفظ تداوم حیات یک موجودیت سایبری و به تبع آن نرم‌افزارها و اطلاعات پایه‌ای آن. مورد ب بدین معنی است که در زمان ناسازگاری فضای سایبری با مؤلفه‌های قدرت (ایدئولوژی، سیاست بدنه و زیرساخت بدنه) یک نهاد سایبری، این نهاد باید بتواند اجرای کار را متوقف کرده و پس از بهبود شرایط مجدداً به عملیات ادامه دهد.

جنبه اول مقاومت، از طریق بهره‌برداری از زیرساخت‌های فیزیکی و سایبری به دست می‌آید. برای تحقق این امر، زیرساخت‌ها باید وجود داشته باشند و منابع باید مقاوم و متناسب با تغییرات فناورانه باشند. به‌طور کلی، محیط باید آمادگی لازم را برای حفظ قدرت سایبری به منظور حفظ ایدئولوژی، سیاست‌های بدنه خود و تأثیرگذاری کافی در چهار بعد قدرت داشته باشد. دستیابی به سطح اول مقاومت نیاز به قدرت سایبری برای ایجاد و حفظ اتحاد و روابط تجاری با قدرت‌های دیگر، از جمله بازیگران غیردولتی مانند نهادهای تجاری دارد. اتحادیه‌ها حفاظت، امنیت و ثبات را فراهم می‌کنند. حفاظت از تمامی مؤلفه‌های یک نهاد سایبری ضروری است و

می‌تواند خروجی کار اتحادیه‌ها باشد. دارایی‌های سایبری می‌تواند به وسیله فناوری‌هایی مانند رمزنگاری، انسداد، تکرار، توزیع، قابل حمل بودن و پنهان شدن محافظت شود. رمزنگاری و انسداد می‌تواند باعث حفاظت از مراکز ارائه و تولید محصولات و خدمات مجازی شود و تکرار و توزیع دارایی‌های سیار، موجب بهبود تداوم کسب‌وکار می‌شود.

جنبه دوم مقاومت، نرم‌افزار و داده‌های یک موجودیت سایبری است که برای تداوم حیات آن ضروری است. نکته مهم این است که با استفاده از روش‌های فناورانه و سایر ابزارها اطمینان حاصل شود که هیچ‌گاه هیچ‌یک از نسخه‌های کد و داده‌ها به طور تصادفی یا عمدی از بین نمی‌روند. استقامت واقعی نیز بدان معنی است که مؤلفه کلیدی سیاست بدنه باید به نحوی پایدار بمانند، که پس از یک دوره ناهنجاری شدید سایبری، مجدداً راه‌اندازی شود.

• انعطاف پذیری

فضای سایبری حوزه بسیار پویا و ناپایداری است. به طور مثال قطع برق می‌تواند زیرساخت را قطع کرده و بلایای طبیعی، حوادث، خطاهای انسانی و اعمال مخرب بخش‌هایی از زیرساخت را غیر فعال سازد. انعطاف‌پذیری یکی دیگر از ویژگی‌های قدرت سایبری است که به عنوان توانایی یک سیستم برای مقاومت، جذب، بهبود یا موفقیت در صورت تغییر در محیط و شرایط تعریف می‌شود.

برای اینکه یک قدرت سایبری به انعطاف‌پذیری رسد، تمام مؤلفه‌های تشکیل‌دهنده آن باید انعطاف‌پذیر باشند. بنابراین، ایدئولوژی، زیرساخت‌های سیاسی، فیزیکی و سایبری باید در برابر اختلال مقاوم باشد و در صورت بروز هرگونه اختلال، بهبودیافته و مجدداً به فعالیت خود ادامه دهد. علاوه بر این، با توجه به نقش اساسی اقتصاد سایبری در حیات قدرت سایبری، انعطاف‌پذیری آن نیز بسیار مهم است.

ایدئولوژی نبض قدرت سایبری است. ایدئولوژی باید دارای یک پایه قانونی ثابت بوده و برای سیاست بدنه جذابیت داشته باشد. ایدئولوژی انعطاف‌پذیر، سازگار با محیط‌های فیزیکی، سایبری و انسانی است. همین امر در مورد یک جنبش سیاسی انعطاف‌پذیر که شامل حاکم و اعضای آن می‌باشد، نیز صدق می‌کند. ابعاد حکومت باید به صورت دوره‌ای از لحاظ اثربخشی و سازگاری بر اساس محیط و با در نظر گرفتن ذینفعان اصلی ارزیابی شود. افراد عضو باید انسجام داشته و به ایدئولوژی و حکومت متعهد باشند. عضویت نباید ایستا باشد بلکه لازم است فرهنگ عضویت به طور مداوم تجدید و نوسازی شود. چنین فرهنگی، عضو را قادر می‌سازد تا بلافاصله بعد از اختلال، ادامه حیات داده و با تغییرات پیش‌بینی نشده و بازسازی نهادهای سایبری سازگار شود.

زیرساخت‌های فیزیکی و سایبری نیز باید انعطاف‌پذیر طراحی شوند. این کار شامل چندین جنبه، از جمله افزونگی، پشتیبان

گیری و انعطاف‌پذیری است. علاوه بر این، به منظور به حداقل رساندن نقاط شکست^۱ باید از اتصال سست^۲ (که در آن یک شکست در یک گره به گره‌های دیگر نفوذ نمی‌کند) استفاده نمود. زیرساخت‌ها باید به گونه‌ای طراحی شوند که در صورت اختلال در یک یا چند گره، کل زیرساخت از کار نیفتد.

تنوع و افزونگی، برای انعطاف‌پذیری اقتصادی ضروری است. بدین معنی که لازم است به منظور جلوگیری از وابستگی به یک نهاد واحد، چندین تأمین‌کننده، تولیدکننده و مصرف‌کننده در هر بخش اقتصادی شرکت کنند. اتصالات بین بخش‌ها باید اتصالات سست بوده تا از اختلالات آبخاری بین بخش‌ها جلوگیری کند. همچنین، روابط تجاری قوی و انعطاف‌پذیر باید بین دولت‌های بزرگ و نهادهای دولتی در اقتصادهای محلی، منطقه‌ای و جهانی وجود داشته باشد.

• وابستگی متقابل

وابستگی متقابل به معنی روابط همزیستی یک نهاد با سایرین، امری است که به نهادهای حقیقی اعم از دولت ملی و همچنین بازیگران غیردولتی کمک می‌کند که در سلسله مراتب قدرت جهانی قرار گیرند. این امر به ویژه برای روابط اقتصادی، دیپلماتیک و نظامی مهم است. به دلیل ماهیت پراکنده و توزیع شده فضای سایبری و همبستگی بین جوامع در این فضا، وابستگی متقابل در معادله قدرت

1.SinglePiont
2.Loosed Couple

همبستگی بین جوامع در این فضا، وابستگی متقابل در معادله قدرت از اهمیت ویژه ای برخوردار است.

وابستگی اقتصادی در جهان فیزیکی و همچنین در دنیای سایبری مشهود است. در دهه ۱۹۸۰، ایالات متحده به دنبال سرمایه از ژاپن برای تعادل بودجه فدرال بود؛ ژاپن به این درخواست رسیدگی کرد زیرا برای صادرات نیاز به اقتصاد قوی ایالات متحده داشت. در حال حاضر، یک رابطه مشابه بین ایالات متحده و چین وجود دارد. پرداخت‌های ایالات متحده در قبال واردات از چین به دلار است. چین می‌تواند دلارهای خود را به فروش برساند تا اقتصاد ژئوپلیتیک رقیب خود را تحت تأثیر قرار دهد، اما انجام این کار موجب تضعیف دلار و کاهش ارزش سهام چین خواهد شد. این امر همچنین می‌تواند صادرات چین را به ایالات متحده کاهش دهد که اقتصاد چین را تضعیف می‌کند. البته وابستگی متقابل می‌تواند اثرات منفی نیز داشته باشد. بحران مالی سال ۲۰۰۸ در ایالات متحده آغاز شد، اما روابط اقتصادی قوی با دیگر کشورها باعث بحران‌های مشابه در اروپا و آسیا شد و در نهایت منجر به رکود جهانی شد.

همبستگی قوی در حال حاضر در اقتصاد سایبری وجود دارد. اشخاصی که در اقتصاد سایبری هستند لزوماً به یکدیگر مرتبط هستند - تولیدکنندگان و مصرف‌کنندگان باید در هر اقتصاد با یکدیگر همکاری کنند. از آنجایی که هر نهاد دارای جوه دنیای سایبری و فیزیکی است، روابط تنگاتنگ میان اقتصادهای سایبری و فیزیکی نیز وجود

دارد. وابستگی اقتصادی در فضای مجازی بسیار حائز اهمیت است. موجودیت‌هایی که دارای تأثیرگذاری زیادی بر فضای مجازی هستند، بدون یک اقتصاد سایبری قوی، که ثبات و انعطاف‌پذیری آن‌ها را بهبود می‌بخشد، قادر به اجرای عملیات‌ها و فعالیت‌های خود نخواهند بود.

در دنیای فیزیکی، وابستگی متقابل بین ابعاد دیپلماتیک و نظامی برای ثبات امنیت نهادهای کوچک‌تر، از جمله بازیگران غیردولتی که برای حفاظت از خود به ملت‌ها متکی هستند، حیاتی است. انتقال قدرت از دنیای فیزیکی به فضای مجازی باعث می‌شود تا انجام دیپلماسی و مشارکت در برنامه‌ریزی برای کسب و ارتقاء قدرت توسط نهادهای کوچک‌تر، حتی بازیگران غیردولتی، آسان‌تر شود. نهادهای کوچک سایبری، بدون نیاز به زیرساخت‌های قابل توجه، قادر به ایجاد محیط‌های پایدار و محرمانه هستند. قدرت‌های بزرگ نیز روابط با نهادهای کوچک‌تر، که می‌توانند فرصت‌های اقتصادی و حمایت دیپلماتیک در زمان‌های متداول در فضای مجازی و جهان فیزیکی فراهم آورند را شکل می‌دهند. بنابراین، وابستگی متقابل باعث ایجاد ثبات در محدوده بسیار پویای فضای مجازی شده و به سایر ویژگی‌های مهم قدرت سایبری مانند ثبات، مقاومت و انعطاف‌پذیری کمک می‌کند.

۳-۴- چارچوب فضای سایبری (دیدگاه David Clark)

با توسعه رویکرد ارائه شده توسط دیوید کلارک^۱ در سال ۲۰۱۰، چهار لایه برای فضای سایبری پیشنهاد شد که در شکل ۱-۶ آمده است.

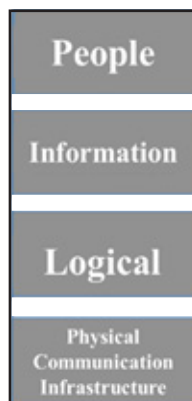
• لایه فیزیکی - ارتباطات - زیرساخت^۲: این لایه از مولفه های لایه منطقی پشتیبانی می کنند.

• لایه منطقی^۳: عبارت است از ساختارهای منطقی که خدمات را می سازند و از ماهیت پلتفرمی فضای سایبری پشتیبانی می کنند.

• لایه اطلاعات^۴: منظور، اطلاعاتی است که در فضای سایبری ذخیره، منتقل و تبدیل می شوند.

• لایه افراد^۵: منظور از افراد کسانی هستند که در فضای سایبری و تجربیات این محیط مشارکت نموده و با اطلاعات کار کرده و با یکدیگر ارتباط برقرار نموده، تصمیم گیری کرده و طرح ها را پیش می برند و ماهیت فضای سایبری را با کار کردن با مولفه های خدمت و قابلیت های آن تغییر می دهند.

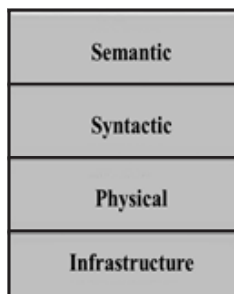
1.David Clark
2.Physical-Communication-Infrastructure
3.Logical
4.Information
5.People



شکل ۴-۲- چارچوب فضای سایبر از دیدگاه David Clark - ۲۰۱۰

۴-۴- چارچوب فضای سایبری (دیدگاه Sheldon)

با توسعه رویکرد ارائه شده توسط شلدون^۱، که بر اساس توسعه چارچوب کلارک ارائه شده است، چهار لایه برای فضای سایبری پیشنهاد می‌گردد که در شکل ۷ ارائه شده است. این لایه‌ها عبارت‌اند از زیرساخت، فیزیکی، ساختاری و معنایی.



شکل ۴-۳- چارچوب فضای سایبری از دیدگاه شلدون - ۲۰۱۱

1.Sheldon

لایه زیرساخت: زیرساخت فضای سایبری شامل سخت‌افزار، سرورها، مؤلفه‌های شبکه، کابل کشی، ماهواره‌ها و سایر تجهیزات است. این لایه می‌تواند با شاخص‌هایی نظیر نسبت جمعیت دارای دسترسی به اینترنت، بازه زمانی که کاربران، سخت‌افزار را ارتقاء می‌دهند، سطح مالکیت اسمارت فون‌ها و تعداد ISP^۱ ها نسبت به جمعیت و تعداد گذرگاه‌های بین‌المللی ارائه‌دهنده اتصالات سراسری اندازه‌گیری شود.

لایه فیزیکی: شامل ابزارهایی مانند PC^۲ ها، لپ‌تاپ‌ها، تبلت‌ها و اسمارت فون‌ها است که کاربران با استفاده از آنها آن با یکدیگر تعامل می‌کنند. شاخص‌های اندازه‌گیری این لایه می‌تواند نسبت بکارگیری کابل مسی در مقایسه با کابل‌های فیبر نوری با سرعت بالا، تعداد نقاط نقاط Wi-Fi در هر جمعیت، پوشش تلفن همراه، متوسط مصرف داده‌ها توسط هر مشترک و هزینه دسترسی در مقایسه با حقوق متوسط ملی باشند.

لایه ساختاری^۳: وظایف این لایه عبارت است از نحوه ساختاردهی به داده‌ها جهت تسهیل ارتباط بین اجزای تشکیل‌دهنده و درون لایه زیرساخت که شامل پروتکل‌های ارتباطی، اجزای نرم‌افزاری و الگوریتم‌های مسیریابی شبکه می‌باشد. شاخص‌های اندازه‌گیری این لایه شامل سطح رمزنگاری داده‌ها، نسبت کامپیوترهای محافظت شده توسط آنتی‌ویروس و سطح دستگاه‌های آلوده، درجه اولویت‌بندی شبکه (بی‌طرفی شبکه) و تعداد ثبت‌نام دامنه باشد.

1. Internet Service Providers

2. Personal Computers

3. syntactic

لایه معنایی^۱: این لایه امکان درک اطلاعات را به کاربران می دهد تا به شکل مفید از آن بهره گیری نمایند و شامل عناصری مانند نوع و محبوبیت رابط کاربر، نرم افزار کاربردی و همچنین ملاحظات زبانی، فرهنگی و فکری است که در طراحی آن ها مورد استفاده قرار می گیرد. شاخص های اندازه گیری این لایه عبارت اند از نسبت تولید ناخالص داخلی از تجارت آنلاین، درصد صفحات وب تولید شده در زبان بومی، درصد کاربران فعال شبکه های اجتماعی به جمعیت، سطح جرائم اینترنتی و میزان اثربخشی قانون و اجرای آن.

بخش پنجم

مدل بلوغ امنیت سایبری



بخش پنجم

مدل بلوغ امنیت سایبری

زیرساخت های فناوری، دارایی های حیاتی برای امنیت عمومی، رفاه اقتصادی و امنیت ملی کشور هستند. سیستم های سایبری به طور گسترده ای برای نظارت و کنترل زیرساخت های حیاتی استفاده می شوند. امنیت سایبری یکی از اهداف مهم برنامه امنیت ملی یک کشور است. تحقیقات محدودی در ارتباط با امنیت سایبری و ارزیابی بلوغ ملی سایبری آغاز شده است. برخی از آن ها به ارزیابی بلوغ تلاش های ملی در رابطه با زیرساخت های مهم اختصاص یافته است. ولی اکثر آن ها صرفاً بررسی شیوه های مختلف امنیتی در سطح ملی در برابر جرائم سایبری و در مورد حفاظت از حریم خصوصی است. این کتاب یک مدل بلوغ برای اندازه گیری سطح آمادگی تلاش های حفاظت ملی از زیرساخت های مهم را پیشنهاد می کند. توسعه این مدل شامل دو مرحله است. در اولین قدم، داده های مربوط به پروژه های امنیت ملی سایبری با استفاده از نظریه های مبتنی بر تجزیه و تحلیل عوامل مؤثر بر حساسیت زیرساخت های بحرانی

به تهدیدات اینترنتی تحلیل می شود. در گام دوم معیارهای بلوغ با معرفی علل ریشه ای به کارشناسان موضوعی در نظرسنجی دلفی تعیین می گردد. مدل بلوغ مبتنی بر نظرسنجی برای ارزیابی تلاش های محافظت از زیرساخت های بحرانی در ترکیه نیز مورد استفاده قرار گرفته شده است و نتایج آن نشان می دهد که مدل بلوغ برای ارزیابی آمادگی حفاظت از زیرساخت های مهم ملی در کشورهای در حال توسعه مانند ترکیه سودمند است.

جدول ۵-۱: خلاصه ای از مدل های بلوغ قدرت سایبری

منبع داده ها برای ارزیابی کشور	اساس معیار ارزیابی	موضوع اصلی	توضیحات	توسعه دهنده	مدل
مقامات دولتی	مشخص نشده	امنیت سایبری	مدل بلوغ جامع برای تعیین موقعیت های امنیتی سایبری سازمان ها، جوامع و ملل	دانشگاه تگزاس در Antonio آمریکا	مدل بلوغ امنیت جامعه سایبری (CCSMM ^۱)
ارزیابی سطح کشور انجام نمی شود	استاندارد ۲۷۰۰۲ و اتحادیه بین المللی مخابرات	امنیت سایبری	مدل جامع امنیت سایبری برای کشورها که شامل یک چارچوب، مدل بلوغ، تخصیص نقش و راهنمای پیاده سازی است	دانشگاه Souissi مراکش	مدل بلوغ امنیت ملی سایبری (NCSecMM ^۲)
منابع عمومی	مشخص نشده	امنیت سایبری	نمره کشور (۳۵ کشور)	شرکت خصوصی Hathaway Global Strategies	شاخص ارزیابی سایبری
پایگاه های اتحادیه بین المللی ارتباطات بین المللی، منابع عمومی و ملی (۹۰ کشور)	برنامه جهانی امنیت اطلاعات در اتحادیه ارتباطات بین المللی	امنیت سایبری	نمره دهی و مرتب سازی کشور (۱۰۴ کشور)	اتحادیه بین المللی International Telecommunication Union	شاخص امنیت جهانی سایبری

1. Community Cyber Security Maturity Model
2. National Cyber Security Maturity Model

مدل	توسعه دهنده	توضیحات	موضوع اصلی	اساس معیار ارزیابی	منبع داده‌ها برای ارزیابی کشور
بلوغ سایبری در منطقه آسیا و اقیانوسیه	سازمان غیردولتی در استرالیا	رتبه‌بندی و مرتب‌سازی کشور (۱۸ کشور)	امنیت سایبری	نظر خبرگان	سهمداران (۱۴ کشور)
مدل بلوغ امنیت ملی سایبری (NCSecMM ^۲)	شرکت خصوصی Booz Allen Hamilton	رتبه‌بندی و مرتب‌سازی کشور (۱۹ کشور)	قدرت سایبری	مشخص نشده	داده‌های منابع عمومی، سازمان‌های بین‌المللی و واحد اطلاعات آکونومیس

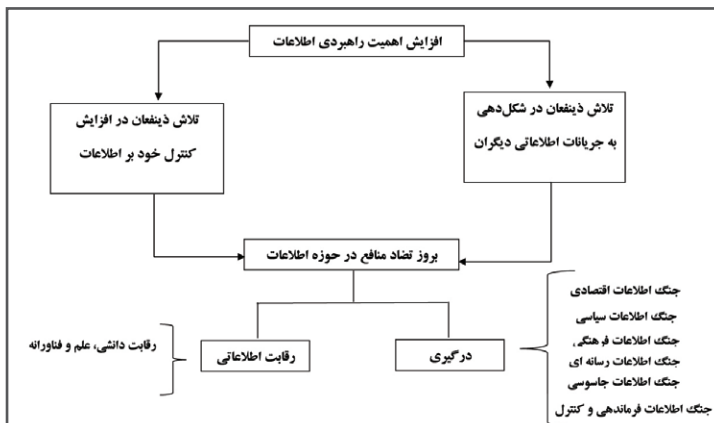
۱-۵- مسئولیت‌ها و نسبت‌ها در فضای سایبری

در ادبیات دانشگاهی، مسئله شناسایی مسئولان و بازیگران حملات سایبری و عدم قطعیت در این موضوع به عنوان یک چالش جدی نگریسته می‌شود و تحقیقات در این زمینه همچنان ادامه دارد. شواهد نشان می‌دهد که حملات سایبری با انگیزه‌های فنی، حقوقی و سیاسی صورت می‌گیرد. نمی‌توان به اتهامات مربوط به حملات سایبری با اطمینان کامل اشاره کرد. بنابراین همواره ممکن است که طرف متهم همان مهاجم واقعی باشد. با توجه به این عدم قطعیت و سایر ویژگی‌های فنی، دولت‌ها تمایلی به پذیرش مسئولیت فعالیت‌های سایبری از سرزمین‌هایشان ندارند (جنسن، ۲۰۱۵).

مسئولیت‌پذیری یکی دیگر از پیش‌شرط‌های لازم برای یک دولت است تا بتواند از حق خود دفاع کند. چالش‌های مربوط به نسبت دادن و پذیرش مسئولیت به دلیل اینکه داده‌ها به صورت تصادفی از یک روتر به روتر دیگر می‌روند، باعث می‌شود دولت‌ها از پذیرش

مسئولیت اجتناب کنند. درعین حال، دولت‌ها نگران فعالیت‌های سایبری مخرب هستند که از طریق زیرساخت‌هایشان عبور می‌کنند. مسئله پذیرش مسئولیت این فعالیت‌ها با وجود بازیگران غیردولتی پیچیده‌تر می‌شود. وجود این بازیگران عدم اطمینان بیشتری ایجاد می‌کند، زیرا دولت‌ها می‌توانند چنین بازیگرانی را برای حمله به یک دولت دیگر استخدام یا تأمین مالی کرده یا آموزش دهند (استاهل^۱، ۲۰۱۱، لاتریونتی^۲، ۲۰۱۳).

در حقوق بین‌الملل، مسئله بازیگران غیردولتی که مرتکب اقدامات مخرب علیه یک دولت دیگر می‌شود، مسئله‌ای پیچیده برای فضای مجازی است. زیرا مسئولیت دولت برای کنترل یا کمک به بازیگران غیردولتی را افزایش می‌دهد.



شکل ۵-۱- الگوی مفهومی مناقشات در عصر اطلاعات

1. Stahl
2. Lotrionti

مسئله دیگر در فضای مجازی این است که چگونه دولت‌های قربانی می‌توانند به بازیگران غیردولتی واقع در قلمرو یک کشور دیگر دسترسی داشته باشند. این مسئله به مسئله مسئولیت پذیری دولت و کنترل دولت بر بازیگران غیردولتی گره خورده است (لاتریونتی، ۲۰۱۳). برخی از دولت‌ها از طریق محدود کردن دسترسی به محتوای اینترنت در سرزمین‌های خود حاکمیت بیشتری در فضای مجازی دارند. بعضی از کشورها، از جمله چین، تصمیم به فیلتر بخشی از محتوای خاص اینترنت که ممکن است به مردم آسیب برساند، گرفته‌اند (لاتریونتی، ۲۰۱۳). در حالی که این امر حاکمیت یک دولت بر قلمرو خود را نشان می‌دهد و تأثیر سیاسی بر روابط بین‌الملل نیز دارد. به عقیده دمچاک^۱ و دامبروسکی^۲ (۲۰۱۳)، این چنین رفتارهایی، شواهدی از سیستم وستفالی در حال توسعه در فضای مجازی می‌باشند. در شکل ۸ الگوی مفهومی مناقشات در عصر اطلاعات نشان داده شده است.

۲-۵- حاکمیت و برابری در فضای سایبری

فضای سایبری نه تنها اصول حقوق بین‌الملل، بلکه اصل حاکمیت دولتی را نیز به چالش می‌کشد و بخشی از مباحث علمی این حوزه، مربوط به وجود و شناخت حاکمیت دولتی در فضای مجازی است. محققان بر این باورند که به دلیل اینکه وجود زیرساخت‌های فیزیکی برای عملکرد فضای مجازی ضروری است، حاکمیت دولتی

1. Demchak
2. Dombrowski

در فضای مجازی نیز وجود داشته و بنابراین حاکمیت در فضای مجازی را به عنوان گسترشی از اصل حاکمیت (فرانزس، ۲۰۰۹؛ لریونته، ۲۰۱۳) در نظر گرفته‌اند.

در حقوق بین‌الملل، حاکمیت یک دولت، حقوق و تعهدات آن دولت را تعریف می‌کند. شناخت حاکمیت دولت‌ها در فضای مجازی به اصل برابری هم مربوط است. بدین معنی که دولت‌ها باید با هم برابر در نظر گرفته شوند. از این‌رو، احترام به اصل برابری، احترام کشورها به حاکمیت یکدیگر را سبب می‌شود (فرانزس، ۲۰۰۹ و جنسن، ۲۰۱۵).

در سطح بنیادی تر، فناوری اطلاعات می‌تواند باعث تغییر و بازآرایی سیاسی در یک کشور و همچنین بین دولت‌ها شود. قدرت اطلاعاتی در دستان افراد، به عنوان رقیبی برای قدرت دولت-ملت‌ها به حساب می‌آید. اطلاعات می‌تواند به طور مؤثری مانع جنگ شده یا آن را تقویت و تشدید نموده و جهت تکامل یا تخریب هر جامعه‌ای به کار رود.

امروزه بسیاری از قدرت پژوهان نسبت به صحت و کارایی معیارهای مورد استفاده در ارزیابی توان و قدرت ملی دچار تردید شده‌اند. این معیارها که عموماً بر متغیرهای مجزا مانند اندازه جمعیت، تولید ناخالص ملی، اندازه نیروهای مسلح، وسعت سرزمین، دسترسی به منابع قابل بهره برداری و تولید فولاد، غلات و غیره متمرکز می‌باشند، هنوز نتوانسته است جزییات مهمی را در مورد قابلیت‌های

یک کشور مشخص در سیاست جهانی فراهم آورد. مجموعه دارایی‌های در اختیار یک کشور فی‌الذاته عنصری از قدرت ملی آن کشور نیست، بلکه عنصری از توان ملی آن کشور است. تجلی قدرت در توان نیست. بلکه قدرت، در صورت امکان به‌کارگیری توان به منظور ایجاد تغییر در محیط متجلی می‌شود. صرفاً از طریق برآورد دقیق منابع گوناگون اقتصادی، سیاسی، نظامی، فرهنگی، اطلاعاتی، سرزمینی، جمعیتی و غیره نمی‌توان قدرت ملی را محاسبه نمود بلکه باید چرخه یا نحوه به‌کارگیری این منابع را که توسط راهبردها، مفاهیم و روابط درون آن کشور مشخص می‌شوند، نیز مورد بررسی قرار داد. در یک رویکرد، قدرت ملی، مجموعه قابلیت‌های بالفعل ملی یک کشور است که بتواند در راستای تأمین منابع ملی، تغییرات دلخواه را در محیط (منابع) و دیگران (رفتار) ایجاد نماید.

با ورود به عصر فناوری اطلاعات، اقتصاد از انحصار دولت‌ها خارج شده است. بنابراین یکی از منابع قدرت از کنترل لایه حکومت خارج شده و کنترل بخش اعم این منابع قدرت توسط بخش غیردولتی باعث سوق یافتن جریان فراوانی از قدرت به خارج از محدوده کنترل شده است. بخشی از جریان قدرت در حال خروج از سیطره نفوذ دولت‌ها بوده و به سرعت به کنترل سازمان‌های غیردولتی درمی‌آید. فناوری اطلاعات نقش مردم و ملت‌ها را در جریان قدرت برجسته ساخته و آن‌ها را قادر به اثرگذاری بر جریان‌های

مختلف سیاسی، اقتصادی و حتی امنیتی اثرگذار نموده است. منبع تولید قدرت و شیوه اعمال آن نیز در حال تغییر از روابط بین ساختارها به روابط بین افراد است.

۵-۴- راهبردهای افزایش کارآمدی حاکمیت توسط فناوری اطلاعات و ارتباطات

در این بخش، راهبردهایی که باعث افزایش کارآمدی حوزه حاکمیت شده و از سوی دیگر توسط فناوری اطلاعات و ارتباطات قابل انجامند عنوان می گردد. برقراری هر یک از این عوامل و اهداف، قدمی برای دستیابی به کارآمدی حاکمیتی است.

- ساده سازی و روان سازی خدمات دولتی
 - شفاف سازی و نظارت بر خدمات و فرآیندهای دولتی
 - یکسان سازی و استانداردسازی خدمات دولتی
 - سرعت بخشی خدمات و فرآیندهای دولتی
 - یکپارچه سازی خدمات دولتی
 - خودکارسازی خدمات و فرآیندهای دولتی
 - مسئولیت پذیری، پاسخگویی و اطلاع رسانی
- بخش ها و نهادهای مرتبط بایستی با هدف اصلی تحقق کارآمدی دولت برای تحقق اهداف شش گانه برنامه ریزی نمایند. مهمترین نهاد مرتبط با این هدف، می تواند سازمان مدیریت و برنامه ریزی کشور باشد.

بخش ششم

فضاهای جغرافیایه اعمال قدرت نرم



بخش ششم

فضاهای جغرافیایی اعمال قدرت نرم

علاوه بر تعریف فضای سایبری در لایه های عمودی، می توان از نظر فضای جغرافیایی اعمال حاکمیت، فضاهای نزدیک، متوسط و دور را نیز به صورت افقی در نظر گرفت. اگر مرز جغرافیایی را به عنوان حوزه یا محدوده ای که هر حکومتی امکان اعمال حکمرانی و حاکمیت داشته باشد در نظر بگیریم، آنگاه جغرافیای سایبر را می توان به سه محدوده فضای نزدیک (حوزه یا محدوده ای از فضای مجازی که توسط سازمان های ملی یا دولتی کنترل و حفاظت می شوند)، فضای میانه (حوزه یا محدوده ای از فضای مجازی که طبق قراردادی مشخص، امکان کنترل و حفاظت بر روی آن وجود دارد و توسط شرکت ها یا دولت کشورهای دوست و همکار اداره می شود) و فضای دور (حوزه یا محدوده ای از فضای مجازی که کنترل محلی بر روی آن وجود ندارد و متعلق به کشورهای متخاصم و دشمن است)، تقسیم بندی کرد. شکل ۹ نمونه هایی از این ارتباط را نشان می دهد. تجزیه و تحلیل نقاط قوت و ضعف دشمن در هر یک از این سه حوزه می تواند

اطلاعاتی در مورد بردارهای احتمالی حمله به جامعه هدف و یا دشمن در هر یک از این سه حوزه جغرافیایی جهت کاهش نفوذ و توانایی آن‌ها برای عملکرد آزادانه در فضای مجازی ارائه دهد.

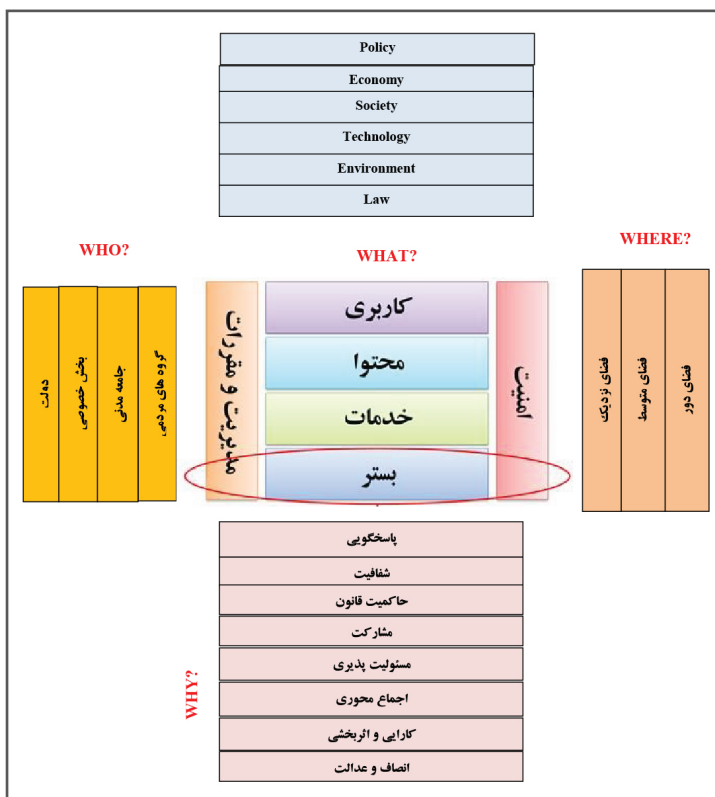


شکل ۶-۱- لایه‌های افقی فضای سایبری

۱-۶- مدل پیشنهادی برای تطبیق و سنجش قدرت نرم در فضای سایبری

تا پیش از توسعه فضای مجازی گستردگی جغرافیایی به‌عنوان یکی از عوامل تعیین‌کننده قدرت ملی محسوب می‌شد، اما در تبیین قدرت سایبری جغرافیا به مفهوم فیزیکی و مصطلح کاربردپذیر نبوده و نیازمند تعریف مجدد است. تحقق قدرت سایبری از تعامل دولت با جامعه مدنی و بخش خصوصی (به‌عنوان بازیگران قدرت ساز)، با در نظر گرفتن مؤلفه‌های تولید قدرت (شامل لایه‌های زیرساخت، منطقی، داده و کاربر) در هر یک از فضاها جغرافیایی قدرت سایبر، امکان‌پذیر است.

در این مدل، حکمرانی به عنوان مجموعه فرآیندهایی که از طریق آن، دولت در تعامل با جامعه مدنی و بخش خصوصی و نهادها در فضاهای مذکور با رعایت اصول حکمرانی خوب چون شفافیت، پاسخ‌گویی، قانون‌گرایی، برابری و جلب مشارکت، همه منابع کشور را در خدمت نفع همگانی و ارتقاء سطح زندگی و رفاه همه مردم قرار داده، مورد استفاده قرار می‌گیرد. در این مدل، مؤلفه‌های قدرت سایبری، بازیگران قدرت ساز آن (دولت، بخش خصوصی و جامعه مدنی)، حوزه‌های اعمال قدرت (فضای نزدیک، میانی و دور)، اهداف (دکترین) حاکمیت (پاسخگویی، شفافیت، حاکمیت قانون، مشارکت، مسئولیت‌پذیری، اجماع محوری، کارایی و اثربخشی و انصاف و عدالت)، نحوه حکمرانی (شاخص‌های مطرح در هر یک از بخش‌های PESTEL)، زمان حکمرانی و میزان حکمرانی به عنوان بخش‌های مطرح، در تقاطع با یکدیگر دیده شده است. با تعیین شاخص‌های تحقق قدرت در حاکمیت از طریق حکمرانی خوب در فضای سایبر، می‌توان نگاهی جامع به زوایای تحقق قدرت در فضای سایبر و به موجب آن قدرت ملی سایبری داشت.



شکل ۶-۲- مدل پیشنهادی برای تبیین قدرت نرم در فضای سایبر

۶-۲- تحلیل مدل پیشنهادی

بر اساس مدل پیشنهادی، تحلیل برخی از گزاره‌ها در قالب این مدل، به صورت زیر پیشنهاد می‌شود:

فضای نزدیک (Where?)				
مؤلفه‌ها (PESTEL)	معیارها	زیرمعیارها (HOW?)	لایه‌های قضای سایر (What?)	بازنگران (WHO?)
Critical Mass (Society)	سطوح آموزشی مهارت‌های فنی	- رشد تولید نیروی کار - افزایش نرخ تحقیق و توسعه به ازای هر میلیون نفر - افزایش سواد و امنیت سایبری، علوم کامپیوتر و مهندسی - گسترش نفوذ آموزش‌ها و شبکه زندگی اسلامی از طریق قضای مجازی	خدمات محصولات	دولت و بخش خصوصی عمرویه‌های مردمی
	تجارت	- افزایش میزان باز بودن تجارت - بررسی نسبت صادرات/ واردات ICT به درصد کل صادرات/ واردات	خدمات هسته	بخش خصوصی و جامعه مدنی دولت و جامعه مدنی
Economic	محیط خلاقانه	- افزایش سهم اقتصاد دیجیتال در اقتصاد کشور - افزایش نسبت سرمایه تحقیق و توسعه به GDP - سرمایه‌گذاری برای افزایش میزان پشته‌های داخلی - به کارگیری و افزایش کارایی یا افزایش تعداد شبکه‌های هوشمند - افزایش ارزش سهام خصوصی و سرمایه‌گذاری به درصد GDP	خدمات محصولات	دولت و عمرویه‌های مردمی بخش خصوصی دولت و بخش خصوصی
	تجارت الکترونیک و حکمرانی	- اعتماد به ایجاد و مدیریت: - حمل و نقل هوشمند - سلامت الکترونیک - سفارشات اینترنتی - اینترنت بانک ...	خدمات کاربردی	دولت و بخش خصوصی

فضای نزدیک (Where?)

دولت و بخش خصوصی	دولت و بخش خصوصی	امنیت	- افزایش امکانات تحقیقاتی - نظامی سایبری - افزایش تعداد مؤسسات آموزشی - جنگ افزارهای سایبری نظامی - افزایش محدوده سایبری برای آموزش - افزایش دسترسی به بازیگران غیردولتی	توسعه ظرفیت سایبری	Economic
دولت و جامعه مدنی	دولت	امنیت	- تأمین پدافند سایبری برای زیرساخت های مهم و حیاتی کشور - ایجاد استراتژی دفاع سایبری - ایجاد یگان های سایبری نظامی (فرماندهی سایبرلانش سایبر) - ایجاد سلاح های سایبر	سایبر و ظرفیت عملکرد هوشمند	Military (Policy)
دولت و جامعه مدنی	دولت و جامعه مدنی	خدمات	- بررسی و مدیریت نفوذ اینترنت / موبایل / شبکه های اجتماعی - بررسی میزان استفاده از هات اسپات wifi به ازای یک میلیارد نفر	دسترسی به فناوری اطلاعات و ارتباطات	Informational (Technology)
دولت و بخش خصوصی	دولت	خدمات هسته	- مدیریت پهنای باند اینترنت - ظرفیت ذخیره، پردازش و صیانت از داده های عظیم ملی	کیفیت فناوری اطلاعات و ارتباطات	Informational (Technology)
دولت و بخش خصوصی	دولت و بخش خصوصی	لایه مدیریت	- ایجاد و مدیریت تعرفه های موبایل و اینترنت پهن باند - افزایش نسبت هزینه فناوری اطلاعات به درصد GDP	بعد اقتصادی فناوری اطلاعات و ارتباطات	Informational (Technology)
دولت و بخش خصوصی	دولت و بخش خصوصی	لایه مدیریت	- تست منظم آسیب پذیری و تاب آوری - محافظت از سخت افزار / نرم افزار	سرورهای امن	Informational (Technology)

۳-۶- شاخص های پیشنهادی برای سنجش قدرت سایبری بر اساس مدل پیشنهادی

همان‌طور که قبلاً هم بحث شد، مدل پیشنهادی در واقع یک مدل بلوغ برای فضای نابالغ سایبری است. برای طراحی راهکارهای دستیابی به قدرت در فضای سایبری، باید برای هر یک از سلول های مدل پیشنهادی که بیانگر المان های مشخصی از لایه فضای سایبری در تقاطع با فضای جغرافیایی اعمال حاکمیت در هر یک از شاخص های PESTEL است، راهکارهای مشخصی در نظر گرفته شده و تعریف مشخصی برای هر یک از شاخص های کلیدی ارائه شود. جدول ۴ نمونه ای از این شاخص ها را در لایه های مبنایی، ساختاری و معنایی در ارتباط با هر یک از فضاها ی جغرافیایی اعمال حاکمیت دور، متوسط و نزدیک نشان می دهد.

جدول ۶-۱ نمونه ای از شاخص ها در لایه مبنایی

شاخص سنجش			لایه	مؤلفه
فضای دور	فضای متوسط	فضای نزدیک		
- میزان وابستگی به تجهیزات دسترسی - تولید کشورهای دشمن / متخاصم	- میزان وابستگی به تجهیزات دسترسی - تولید کشورهای همکار / دوست - میزان واردات تجهیزات اتصال	- میزان بومی بودن تجهیزات دسترسی (موبایل، لپ تاپ، تبلت، IOT) - میزان صادرات تجهیزات اتصال - جمعیتی که دسترسی به اینترنت دارند	۱. زیرساخت	۱. زیرساخت
		بازه زمانی میانگین کاربرانی که سخت افزار را ارتقاء می دهند		۲. زیرساخت
- میزان ترافیک داخلی انتقالی به واسطه زیرساخت کشورهای رقیب/ متخاصم - سطح مالکیت اسمارت فون ها - میانگین سرعت اتصال کاربران - میزان فیبر نوری شبکه - نسبت به کارگیری کابل مسی در مقایسه با کابل های فیبر نوری - سرعت بالا - تعداد نقاط نقاط Wi-Fi در هر جمعیت - پوشش تلفن همراه - متوسط مصرف داده ها در هر مشترک و - هزینه دسترسی در مقایسه با حقوق متوسط ملی - تعداد ISP ها مرتبط با جمعیت - تعداد گذرگاه های بین المللی ارائه دهنده - ارائه دهنده اتصالات سراسری - میزان ترافیک داخلی - نسبت ترافیک داخلی به ترافیک خارجی - نسبت ترافیک داخلی به ترانزیت بین المللی - میزان ترافیک خارجی عبور داده شده از زیرساخت کشورهای همکار / دوست	- میزان ترافیک داخلی انتقالی به واسطه زیرساخت کشورهای همکار / دوست - سطح مالکیت اسمارت فون ها - میانگین سرعت اتصال کاربران - میزان فیبر نوری شبکه - نسبت به کارگیری کابل مسی در مقایسه با کابل های فیبر نوری - سرعت بالا - تعداد نقاط نقاط Wi-Fi در هر جمعیت - پوشش تلفن همراه - متوسط مصرف داده ها در هر مشترک و - هزینه دسترسی در مقایسه با حقوق متوسط ملی - تعداد ISP ها مرتبط با جمعیت - تعداد گذرگاه های بین المللی ارائه دهنده - ارائه دهنده اتصالات سراسری - میزان ترافیک داخلی - نسبت ترافیک داخلی به ترافیک خارجی - نسبت ترافیک داخلی به ترانزیت بین المللی - میزان ترافیک خارجی عبور داده شده از زیرساخت کشورهای همکار / دوست	- سطح مالکیت اسمارت فون ها - میانگین سرعت اتصال کاربران - میزان فیبر نوری شبکه - نسبت به کارگیری کابل مسی در مقایسه با کابل های فیبر نوری - سرعت بالا - تعداد نقاط نقاط Wi-Fi در هر جمعیت - پوشش تلفن همراه - متوسط مصرف داده ها در هر مشترک - هزینه دسترسی در مقایسه با حقوق متوسط ملی - تعداد ISP ها مرتبط با جمعیت - تعداد گذرگاه های بین المللی ارائه دهنده - ارائه دهنده اتصالات سراسری - میزان ترافیک داخلی - نسبت ترافیک داخلی به ترافیک خارجی - نسبت ترافیک داخلی به ترانزیت بین المللی	۲. زیرساخت	۲. زیرساخت
- میزان ترافیک داخلی انتقالی به واسطه زیرساخت کشورهای رقیب/ متخاصم - سطح مالکیت اسمارت فون ها - میانگین سرعت اتصال کاربران - میزان فیبر نوری شبکه - نسبت به کارگیری کابل مسی در مقایسه با کابل های فیبر نوری - سرعت بالا - تعداد نقاط نقاط Wi-Fi در هر جمعیت - پوشش تلفن همراه - متوسط مصرف داده ها در هر مشترک و - هزینه دسترسی در مقایسه با حقوق متوسط ملی - تعداد ISP ها مرتبط با جمعیت - تعداد گذرگاه های بین المللی ارائه دهنده - ارائه دهنده اتصالات سراسری - میزان ترافیک داخلی - نسبت ترافیک داخلی به ترافیک خارجی - نسبت ترافیک داخلی به ترانزیت بین المللی - میزان ترافیک خارجی عبور داده شده از زیرساخت کشورهای همکار / دوست	- میزان ترافیک داخلی انتقالی به واسطه زیرساخت کشورهای همکار / دوست - سطح مالکیت اسمارت فون ها - میانگین سرعت اتصال کاربران - میزان فیبر نوری شبکه - نسبت به کارگیری کابل مسی در مقایسه با کابل های فیبر نوری - سرعت بالا - تعداد نقاط نقاط Wi-Fi در هر جمعیت - پوشش تلفن همراه - متوسط مصرف داده ها در هر مشترک و - هزینه دسترسی در مقایسه با حقوق متوسط ملی - تعداد ISP ها مرتبط با جمعیت - تعداد گذرگاه های بین المللی ارائه دهنده - ارائه دهنده اتصالات سراسری - میزان ترافیک داخلی - نسبت ترافیک داخلی به ترافیک خارجی - نسبت ترافیک داخلی به ترانزیت بین المللی - میزان ترافیک خارجی عبور داده شده از زیرساخت کشورهای همکار / دوست	- سطح مالکیت اسمارت فون ها - میانگین سرعت اتصال کاربران - میزان فیبر نوری شبکه - نسبت به کارگیری کابل مسی در مقایسه با کابل های فیبر نوری - سرعت بالا - تعداد نقاط نقاط Wi-Fi در هر جمعیت - پوشش تلفن همراه - متوسط مصرف داده ها در هر مشترک - هزینه دسترسی در مقایسه با حقوق متوسط ملی - تعداد ISP ها مرتبط با جمعیت - تعداد گذرگاه های بین المللی ارائه دهنده - ارائه دهنده اتصالات سراسری - میزان ترافیک داخلی - نسبت ترافیک داخلی به ترافیک خارجی - نسبت ترافیک داخلی به ترانزیت بین المللی		۳. زیرساخت

شاخص سنجش			مؤلفه	لایه
فضای دور	فضای متوسط	فضای نزدیک		
- سطح رمزنگاری که به‌طور معمول استفاده می‌شود، - تعداد استانداردهای کشورهای رقیب - نسبت به استانداردهای بین‌المللی - میزان استفاده از استانداردهای کشورهای رقیب - نسبت به استانداردهای بین‌المللی	- سطح رمزنگاری که به‌طور معمول استفاده می‌شود، - تعداد استانداردهای کشورهای همکار - نسبت به استانداردهای بین‌المللی - میزان استفاده از استانداردهای کشورهای همکار - نسبت به استانداردهای بین‌المللی	- سطح رمزنگاری که به‌طور معمول استفاده می‌شود، - تعداد استانداردهای بومی نسبت به استانداردهای بین‌المللی - میزان استفاده از استانداردهای بومی - نسبت به استانداردهای بین‌المللی	فناوری اطلاعات	تکنولوژی
- تعداد CDN های داخلی - میزان ترافیک CDN های داخلی نسبت به خارجی - تعداد خدمات ابری - میزان استفاده از خدمات ابری کشورهای رقیب - میزان ترانزیت ترافیک بین‌المللی - میزان ترافیک داخلی نسبت به ترافیک خارجی - تعداد شبکه‌های اجتماعی کشورهای رقیب - نسبت به خارجی - تعداد موتور جستجوی کشورهای رقیب - نسبت به خارجی - تعداد رایانامه کشورهای رقیب نسبت به خارجی - تعداد زیر شبکه‌های مستقل داخلی - میزان استفاده از CDN کشورهای رقیب - میزان استفاده خدمات داخلی از خدمات ابری کشورهای رقیب - میزان استفاده کاربران داخلی از موتورهای جستجو، شبکه‌های اجتماعی، رایانامه - کشورهای رقیب	- تعداد CDN های داخلی - میزان ترافیک CDN های داخلی - نسبت به خارجی - تعداد خدمات ابری - میزان استفاده از خدمات ابری کشورهای همکار - میزان ترانزیت ترافیک بین‌المللی - میزان ترافیک داخلی نسبت به ترافیک خارجی - تعداد شبکه‌های اجتماعی کشورهای همکار - نسبت به خارجی - تعداد موتور جستجوی کشورهای همکار - نسبت به خارجی - تعداد رایانامه کشورهای همکار نسبت به خارجی - تعداد زیر شبکه‌های مستقل داخلی - میزان استفاده از CDN کشورهای همکار - میزان استفاده خدمات داخلی از خدمات ابری کشورهای همکار - میزان استفاده کاربران داخلی از موتورهای جستجو، شبکه‌های اجتماعی، رایانامه - کشورهای رقیب	- تعداد CDN های داخلی - میزان ترافیک CDN های داخلی - نسبت به خارجی - تعداد خدمات ابری - میزان استفاده از خدمات ابری - میزان ترانزیت ترافیک بین‌المللی - میزان ترافیک داخلی نسبت به ترافیک خارجی - تعداد شبکه‌های اجتماعی بومی - نسبت به غریبومی - تعداد موتور جستجوی بومی نسبت به غریبومی - تعداد رایانامه بومی نسبت به غریبومی - تعداد زیر شبکه‌های مستقل داخلی		

شاخص سنجش					
لا به	مولفه	فضای نزدیک	فضای متوسط	فضای دور	معنای
شناختی	درون اجزایی	- تعداد پروتکل های بومی نسبت به پروتکل های بین المللی - میزان استفاده از پروتکل های بومی نسبت به پروتکل های بین المللی	- تعداد پروتکل های بومی شده توسط کشورهای همکار - میزان استفاده پروتکل های بومی شده توسط کشورهای همکار	- تعداد پروتکل های بومی شده توسط کشورهای رقیب - میزان استفاده پروتکل های بومی شده توسط کشورهای رقیب	
	نرم افزارهای کاربردی	نسبت برنامه های کاربردی مورد استفاده داخلی نسبت به خارجی	میزان استفاده از نرم افزارهای کاربردی کشورهای همکار توسط کاربران داخلی	میزان استفاده از نرم افزارهای کاربردی کشورهای رقیب توسط کاربران داخلی	
معنایی	بازی های رایانه ای	- تعداد بازی های رایانه ای بومی - نسبت بازی های رایانه ای بومی به خارجی	- تعداد بازی های رایانه ای کشورهای همکار - میزان استفاده از بازی های رایانه ای کشورهای همکار توسط کاربران داخلی	- تعداد بازی های رایانه ای کشورهای رقیب - میزان استفاده از بازی های رایانه ای کشورهای رقیب توسط کاربران داخلی	
	MP	- تعداد MP های بومی - میزان مراجعه به MP های بومی نسبت به خارجی	- تعداد MP های کشورهای همکار - میزان مراجعه به MP های کشورهای همکار	- تعداد MP های کشورهای رقیب - میزان مراجعه به MP های کشورهای رقیب	
	کتابخانه دیجیتال	- تعداد بومی - میزان مراجعه بومی نسبت به خارجی			
	صفحات وب	- تعداد بومی - میزان مراجعه بومی نسبت به خارجی	- تعداد صفحات فارسی ایندکس شده توسط همکار - تعداد صفحات پر مراجعه در کشورهای همکار	- تعداد صفحات فارسی ایندکس شده توسط رقیب - تعداد صفحات پر مراجعه در کشورهای رقیب	

جمع بندی

قدرت و
حاکمیت
سایبری



هدف نهایی قدرت آن است که بتواند رفتار و اعمال دیگران را کنترل کند، حتی اگر برخلاف اراده اش باشد. از دیدگاه سنتی، این موضوع در قدرت سخت با استفاده از اعمال زور و قدرت و با در نظر گرفتن توان بالقوه نظامی و تهدید مطرح شده است. با این حال، قدرت نرم جذابیت آفرینی در فضای سایبری به عنوان یک رویکرد جایگزین یا همراه و بخشی از یک راهبرد قدرت هوشمند و منسجم در نظر گرفته شده است. استفاده از فضای سایبری به عنوان وسیله ای برای طراحی قدرت نرم شامل شناسایی و نقشه برداری از شبکه ها و زیرساخت های مورد استفاده برای رسیدن به مخاطبان مورد نظر و ایجاد یک پیام محرمانه فرهنگی است.

توسعه یک کمپین قدرت نرم یک تعهد چالش انگیز است، زیرا نیاز به درک عمیق از یک محیط پیچیده دارد و برای دستیابی به اثربخشی باید طیف وسیعی از معیارهای اجرایی را در نظر بگیرد. جنبه کلیدی هر فعالیت، نفوذ در فضای مجازی، سنجش میزان نفوذ

پیام در مخاطبان هدف و پاسخ آن‌ها به پیام مورد نظر است. در این زمینه عوامل انسانی نقش مهمی ایفا می‌کنند. روش‌هایی برای اندازه‌گیری انتشار و پاسخ به یک پیام قدرت نرم در جامعه هدف عبارت‌اند از: ترسیم تکنیک‌های مؤثر و بالغ برای اندازه‌گیری مشروعیت تعامل و یا غیرقانونی بودن و توسعه نرم‌افزارهای مخرب. در این گزارش مدل مکعبی از فضای سایبر ارائه شد که می‌تواند برای شناسایی و تحلیل عناصر موردنیاز جهت کنترل قدرت مورد استفاده قرار گیرد تا هدف بتواند با موفقیت انجام شود.

منابع



- [۱] Lister, C. (۲۰۱۴) Profiling the Islamic state. The Brookings Institution, http://www.brookings.edu/~media/Research/Files/Reports/۱۱/۲۰۱۴/profiling۲۰۱۴islamic۲۰۱۴state۲۰۱۴lister/en_web_lister.pdf, accessed ۵ February ۲۰۱۴.
- [۲] Valeriano, Brandon. "Cyber Strategy: The Evolving Nature of Cyber Power and Coercion." Enigma ۲۰۱۸ (Enigma ۲۰۱۸) (۲۰۱۸).
- [۳] Venables, Adrian, Siraj Ahmed Shaikh, and James Shuttleworth. "The projection and measurement of cyberpower." Security Journal ۲۰, no. ۱۰۱۱-۱۰۰۰ : (۲۰۱۷) ۳.
- [۴] Murphy, Dennis M., Jeffrey L. Groh, David J. Smith, and Cynthia E. Ayers. "Information as Pouver: An Anthology of Selected United States Army War College Student Papers." US Army War College, Carlisle Barracks, Pennsylvania ۲۰۰۶) ۱۷۰۱۳).
- [۵] Ghernaouti-Helie, Solange. Cyber power: crime, conflict and security in cyberspace. EPFL Press, ۲۰۱۶.
- [۶] Karabacak, Bilge, Sevgi Ozkan Yildirim, and Nazife Baykal. "A vulnerability-driven cyber security maturity model for measuring national critical infrastructure protection preparedness." International Journal of Critical Infrastructure Protection ۵۹-۴۷ : (۲۰۱۶) ۱۵.
- [۷] Fischerkeller, Michael P., and Richard J. Harknett. "Deterrence is Not a Credible Strategy for Cyberspace." Orbis ۶۱, no. ۳۹۳-۳۸۱ : (۲۰۱۷) ۳.
- [۸] Campbell, Peter. "Generals in Cyberspace: Military Insights for Defending Cyberspace." Orbis ۶۳, no. ۲۷۷-۲۶۲ : (۲۰۱۸) ۲.
- [۹] Rowland, Jill, Mason Rice, and Sujeet Shenoi. "The anatomy of a cyber-power." International Journal of Critical Infrastructure Protection ۷, no. ۱۱-۳ : (۲۰۱۴) ۱.

[۱۰] Rowland, Jill, Mason Rice, and Sujeet Shenoi. "Whither cyberpower?" International Journal of Critical Infrastructure Protection ۷, no. ۱۳۷-۱۲۴: (۲۰۱۴) ۲.

[۱۱] بهروز ثروتی، هادی جمشیدیان (۱۳۸۹)، کتاب "فناوری و قدرت ملی (چالش-ها و راهبردها)"، ناشر: دانشگاه

عالی دفاع ملی، شابک: ۹۷۸-۶۰۰-۵۳۹۱-۳۶-۷

[۱۲] van Vuuren, Joey Jansen, and Louise Leenen. "A Model for Measuring Perceived Cyberpower." In ICCWS ۱۳ ۲۰۱۸th International Conference on Cyber Warfare and Security, p. ۳۲۰. Academic Conferences and publishing limited, ۲۰۱۸.



مرکز ملی فضای مجازی
پژوهشگاه فضای مجازی