Karafan

Quarterly Scientific Journal of Technical and Vocational University

Autumn 2022, Vol. 19, No. 3, p. 501-527

Journal Homepage: https://karafan.tvu.ac.ir/?lang=en

dor:10.48301/KSSA.2022.339869.2083

TVU

A Model for Cyber Power, the Fifth Dimension of National Power

Hamed Sepehrzadeh[1*]

[1]Assistant Professor, Department of Computer Engineering, Technical and Vocational University (TVU), Tehran, Iran.

ARTICLE INFO

Article Type:
Original Research

Received: 05.01.2022
Revised: 08.18.2022
Accepted: 05.28.2022

Keyword:
Cyberspace
Cyber Entity
Cyber Power
Dimensions of Cyber Power
Components of Cyber Power

***Corresponding Author:**
Hamed Sepehrzadeh
Email: *hsepehrzadeh@tvu.ac.ir*

ABSTRACT

The use of cyberspace has become very widespread among communities. With the increase of internet usage in Iran and worldwide in the social, industrial and banking fields, there has been an increase in fear of possible resulting harm. Until now, power was presented in four areas of land, sea, air and space, but today, cyberspace has become one of the main areas of power very distinct from other areas. Cyber power has become one of the foremost concerns in the world and one of the most researched topics in the fields of engineering and science. Cyber power is defined as the ability to use cyberspace to obtain results and make an impact in other operating environments. In this article, a conceptual model for cyber power is presented. To this end, the macro dimensions and components of cyber power were identified. In line with this goal, the main components of these dimensions were identified and the existing challenges and obstacles to establishing cyber power and their solutions were discussed. Distinctive aspects of cyber power with the concept of power in different areas were also discussed. The main purpose of this study was to investigate the dimensions and components of cyber power in order to achieve a conceptual model for cyber power.

E-ISSN: 2538-4430
ISSN: 2382-9796

EXTENDED ABSTRACT

Introduction

Cyberspace is the ever-expanding manifestation of communication and information infrastructures and is a rich environment for exercising power and influence. All institutions including national institutions, private companies and terrorist organizations place vital aspects of their operations in cyberspace to benefit from the benefits provided by that domain. Cyber space is balancing in the sense that it creates a balance in the national power of countries. In fact, cyberspace provides protection and anonymity, and the possibility of using and participating in virtual economies with little cost. This issue fundamentally disrupts power equations. The main goal of this research is to identify the macro dimensions of cyber power and its components. It is essential to identify these dimensions in order to achieve cyber power and create a country's cyber power model.

Methodology

In this section, a conceptual model for cyber power is presented. The distinctive aspect of this research is the introduction of new dimensions and components in the cyber power model which are very important and should not be ignored.

Cultural dimension

In the cultural dimension, issues such as the transfer of values, identity transformations, privacy, creation of new social demands, and generation gap which are related to the layers of users and the content of the cyber space model exist.

Economic dimension

Economic power (or at least economic support by other powers) might be considered as the most important dimension of a cyber power. Without financial resources, a cyber power cannot pursue its ideology, attract people or create infrastructure.

Political and diplomatic dimension

The diplomatic dimension is necessary for the survival of a cyber power. No institution in the real world can work without strong relationships with other institutions. Similarly, a cyber power, however small, must maintain its connections with other powers, real and virtual, for income, resources and diplomatic support, and indeed for its existence.

Information dimension

Cyber espionage is a type of cyber threat which means obtaining confidential information by using the power of technology and without the permission of the owner of the computer facility. Cyber espionage can be done for various reasons or to achieve different goals.

An important point that applies to cyber threats is the role of the internet and the existence of an internet connection for the realization of threats. That is, if the computer devices are not connected to the international space of the internet, the possibility of threats in the described forms is minimized, if not impossible.

Military dimension

In the military aspect, the issue of cyber security becomes very important. Because a country can attack the vital infrastructures of another country through cyber space resulting in destroying cyber space or physical infrastructure. Many researchers define security as the absence of threats, and for this reason, they believe that cyber security is possible in the absence of major cyber threats to systems, as a result of which cyber information protection will be possible.

People dimension

A person plays different roles such as a community member, system user, system information owner, hacker or system information attacker. People are usually known as the weak link in the information security chain.

Content dimension

Cyberspace is a suitable and very effective space for promoting ideology and explaining different views to supporters and opponents. Today, the adoption of the internet and new communication-information technologies has led to the emergence of virtual space alongside the real world, and this has upset the equations and patterns of traditional communication of information production, transmission and consumption resulting in changes.

Critical infrastructure dimension

Cyber-physical systems are integration of computer systems and communication with physical processes. There is consensus that it aims to achieve greater efficiency, reliability and strength of physical systems, but simultaneously has been exposed to new security threats. Unlike cyber systems, infiltrating cyber-physical systems does not necessarily mean destroying them, but the attacker's goal is to cause physical damage and disruption to these systems.

Conclusion

Cyberspace is a new battlefield where network packets can be sent almost instantaneously across the globe to physical systems, including infrastructure systems in the physical and cyber domains. The dimensions of cyber power can be divided into seven cultural, economic, political and diplomatic, informational, military, social and critical infrastructure dimensions. In the cultural dimension, issues such as the transfer of values, identity transformations, privacy, the creation of new social demands, and generation gap are considered related to the layers of users and the content of the cyberspace model. The economic dimension is considered as one of the most important dimensions of cyber power because it has a great impact on the continuity, stability and advancement of its goals and ideals. This dimension is mostly related to the infrastructure and service layers, although it is also related to the user and content layers to some extent. In the political and diplomatic dimension, issues such as facilitation of the globalization plan, control of information, transformation in the concepts of power, guidance and guidance of new political sectors, transformation of the political space in the virtual environment, and fraudulent-political people are deliberated. In terms of content, it is important to promote ideology and explain different points of view to the audience. In the military dimension, the concepts of cyber terrorist, cyber warfare and espionage are expounded on. In the

social dimension, which is one of the most important dimensions, society, cyber awareness and defensive spirit are prominent which are important to safety and environmental, personal, social and financial resources. A person can play different roles such as a community member, system user, system information owner, or hacker and attacker to system information. People are usually known as the weak connection points in the information security chain. Therefore, one of the important characteristics of users that affects the achievement of cyber power is cyber knowledge.

کارافن
فصلنامه علمی دانشگاه فنی و حرفه‌ای
پاییز ۱۴۰۱، دوره ۱۹، شماره ۳، ۵۲۷-۵۰۱
آدرس نشریه: https://karafan.tvu.ac.ir/
doi:10.48301/KSSA.2022.339869.2083

مدلی برای قدرت سایبری؛ بعد پنجم قدرت ملّی

حامد سپهرزاده[1*]

۱- استادیار، گروه مهندسی کامپیوتر، دانشگاه فنی و حرفه‌ای، تهران، ایران.

اطلاعات مقاله

نوع مقاله: مقاله پژوهشی

دریافت مقاله: ۱۴۰۱/۰۲/۱۱
بازنگری مقاله: ۱۴۰۱/۰۲/۲۸
پذیرش مقاله: ۱۴۰۱/۰۳/۰۷

کلید واژگان:
فضای سایبری
نهاد سایبری
قدرت سایبری
ابعاد قدرت سایبری
مؤلفه‌های قدرت سایبری

***نویسنده مسئول:** حامد سپهرزاده
پست الکترونیکی:
hsepehrzadeh@tvu.ac.ir

چکیده

استفاده از فضای سایبری در میان جوامع بسیار فراگیر شده است. با افزایش ضریب نفوذ اینترنت در ایران و جهان در حوزه‌های اجتماعی، صنعتی و بانکی و غیره، نگرانی از صدمات احتمالی نیز افزایش زیادی یافته است. تاکنون قدرت در چهار حوزه زمین، دریا، هوا و فضا مطرح می‌شد اما امروزه فضای سایبری به یکی از حوزه‌های مهم قدرت تبدیل شده است که از جهاتی بسیار با سایر حوزه‌ها متفاوت است. امروزه قدرت سایبری به یکی از مهم‌ترین دغدغه‌های تمام کشورها و یکی از مهم‌ترین موضوعات پژوهشی در حوزه مهندسی و علوم تبدیل شده است. قدرت سایبری، به‌صورت توانایی استفاده از فضای سایبری، برای اخذ نتایج و تأثیر گذاشتن در سایر محیط‌های عملیاتی تعریف می‌شود. در این مقاله قصد داریم به ارائه مدل مفهومی برای قدرت سایبری بپردازیم. به همین منظور، به شناسایی ابعاد کلان و مؤلفه‌های قدرت سایبری خواهیم پرداخت. در راستای این هدف، مؤلفه‌های اصلی این ابعاد شناسایی شده و در مورد مسائل و موانع موجود برای برقراری قدرت سایبری و راه‌حل آن‌ها بحث شده است. همچنین به جنبه‌های متمایز قدرت سایبری با مفهوم قدرت در حوزه‌های مختلف پرداخته شده است. هدف اصلی در این پژوهش، بررسی ابعاد و مؤلفه‌های قدرت سایبری به‌منظور دستیابی به مدل مفهومی برای قدرت سایبری است.

شاپای الکترونیکی: ۲۵۳۸-۴۴۳۰
شاپای چاپی: ۲۳۸۲-۹۷۹۶

مقدمه

فضای سایبری، در حال گسترش از زیرساخت‌های ارتباطی و اطلاعاتی و محیطی غنی برای اعمال قدرت و نفوذ است [۱; ۲]. همه نهادها از هر نوعی، مانند نهادهای ملّی، شرکت‌ها و سازمان‌های تروریستی، جنبه‌های حیاتی از عملکرشان را در فضای سایبری قرار می‌دهند تا از مزایای ارائه شده توسط آن حوزه بهره‌مند شوند. فضای سایبری متعادل‌کننده است [۳] به این معنا که توازنی در مورد قدرت ملّی کشورها ایجاد می‌کند. در واقع فضای سایبری، محافظت و گمنامی و امکان استفاده و شرکت در اقتصادهای مجازی را با هزینه اندک فراهم می‌آورد [۴]. این موضوع به‌طور اساسی معادلات قدرت را بر هم می‌زند [۴].

نکته مهم در تفاوت اعمال قدرت در فضای سایبری و سایر قلمروهای اعمال قدرت مانند دریا و زمین این است که جغرافیایی فضای سایبری، بسیار تغییرپذیر است [۳]. نکته‌ای که باید به آن دقت کرد این است که در قلمروی سایبری، حتی کشورهای کوچک یا گروه‌هایی که وابستگی به دولت‌ها ندارند می‌توانند در سطوحی، به قدرت سایبری برسند [۱].

شناخت فضای سایبری از الزام‌های اولیه و اساسی برای موفقیت در راستای افزایش توان کشور در این حوزه است و به‌واسطه ایجاد این درک، امکان مدیریت ادراک و ترسیم راهبرد امکان‌پذیر خواهد بود. روند تغییر و تحولات سریع عصر حاضر، نشانه‌ای واضح از تغییرها در آینده است و امروزه هیچ کشوری از نفوذ پیشرفت‌های حیرت‌انگیز فناوری ارتباطات مصون نیست. بنابراین لازم است فضای مجازی در ابعاد مختلف فرهنگی- اجتماعی، سیاسی، امنیتی و روان‌شناختی مورد بررسی و توجه قرار گیرد.

جنبه ترسناک سلاح‌های سایبری آسیب‌هایی است که می‌تواند در دارایی‌های زیرساخت‌های حیاتی ایجاد کنند. سلاح‌های سایبری، عدم‌تقارن بزرگی را به جنگ و به تبع آن به ابعاد نظامی قدرت وارد می‌کنند [۴; ۵]. برخلاف حوزه‌های زمین، دریا، هوا و فضا، هر نهاد مدرن باید بتواند سلاح‌های بسیار پیچیده برای استفاده در فضای مجازی توسعه دهد. ملت‌های کوچک با چنین سلاحی و اداره آن در آینده، تهدیدهای قابل‌توجهی را به قدرت‌های بزرگ‌تر وارد می‌کنند. حتی ابرقدرت‌ها هم ممکن است پس از حمله سایبری به زانو در بیایند. یک ابرقدرت وقتی شبکه برق آن به مدت شش ماه از کار بیفتد و تجهیزات هوشمند آن نتواند علّت را شناسایی کند، چه کاری را می‌تواند انجام دهد؟ فضای مجازی به‌طور قابل‌توجهی شکاف قدرت بین کشورها را کاهش می‌دهد. به کشورها توانایی مقابله با قدرت‌های بزرگ را در تمام چهار بعد قدرت می‌دهد [۶; ۷].

هدف اصلی این تحقیق، شناسایی ابعاد کلان قدرت سایبری و مؤلفه‌های آن است. شناسایی این ابعاد در راستای دستیابی به قدرت سایبری و ایجاد الگوی قدرت سایبری کشور بسیار ضروری است. همچنین به جنبه‌های متمایز قدرت سایبری با مفهوم قدرت در حوزه‌های مختلف پرداخته شده است. هدف اصلی بررسی ابعاد و مؤلفه‌های قدرت سایبری به‌منظور دستیابی به الگوی قدرت سایبری است.

در ادامه، در بخش ۲، به پیشینه پژوهش خواهیم پرداخت. در بخش ۳، به تعاریف و توضیح مفاهیم مبنایی قدرت سایبری متمرکز می‌شویم. در بخش ۴، به معرفی ابعاد کلان و مؤلفه‌های یک قدرت سایبری می‌پردازیم. در بخش ۵ نیز نتایج حاصل از پژوهش ارائه شده است.

پیشینه پژوهش

در [۲] نویسندگان ضمن معرفی ویژگی‌های فضای سایبر، وضعیت کشور را براساس آمارهای موجود ارزیابی کرده‌اند و پس از بررسی مسئله امنیت فضای سایبری، به اولویت‌بندی در استقرار آن پرداخته است. همچنین دولت الکترونیکی به‌عنوان مهم‌ترین ره‌آورد فضای سایبر بررسی شده است. در [۸] نویسندگان به مقایسه روش‌های شناسایی رفتار کارمندان داخلی در فرایند حمله به سیستم‌های رایانه‌ای پرداخته‌اند. آن‌ها نشان دادند که حملات کارمند داخلی بسیار

پیچیده است؛ زیرا کارمند داخلی با داشتن اطلاعات و مهارت‌های لازم دسترسی‌ها دانش نسبی از نقاط ضعف و آسیب‌پذیری‌های سیستم‌های امنیتی سازمان و ویژگی‌های فردی که می‌تواند انگیزه‌ای برای ارتکاب حمله باشد امکان انجام هرگونه عمل مخربی را دارد.

در [۹] نویسندگان به ارائه یک مدل تعالی برای مدیریت امنیت اطلاعات در سازمان‌ها پرداخته‌اند. آن‌ها نشان دادند که مسائل امنیتی کارکنان از استخدام و اخراج گرفته تا آموزش و آگاهی آنان نقشی حیاتی در عملکرد پیشگیرانه و دفاعی سازمان دارند. نتیجه‌گیری نهایی بیان می‌کند که اگر شما قانون‌شکنی‌ها و تخلفات رایانه‌ای را طی چند دهه اخیر بررسی کنید، یک ویژگی مشترک در آن‌ها می‌بینید: همه آن‌ها توسط افراد به وقوع پیوسته‌اند. عوامل نفوذ، افراد بوده‌اند، ویروس‌های رایانه‌ای را افراد نوشته بودند و رمزهای عبور را نیز افراد دزدیده بودند؛ بنابراین رابطه مستقیم تعالی سازمانی و امنیت کارکنان سازمان، تقدم و تأخر هرکدام به‌خوبی تبیین می‌شود.

در [۱۰] نویسندگان به بیان تهدیدات و مسائل، تنگناها و تهدیدات در فضای سایبری پرداخته‌اند و جنبه‌های مختلف این تهدیدات و مسائل را بررسی کرده‌اند. نویسندگان در [۱۱] سیاست‌های کنترل دسترسی به داده‌ها برای افزایش محرمانگی داده‌ها را بررسی کرده‌اند. راه‌حل آن‌ها به‌روزرسانی سیاست‌های دسترسی کاربر با هزینه کمی از توان محاسباتی و تعداد کلیدهای محرمانه کاربر را هدف قرار داده است. در [۱۲] نویسندگان به بررسی جنبه‌های حقوقی حملات سایبری پرداخته‌اند و در [۱۳] نویسندگان به بررسی الگوریتم‌های پیشگیری از لو رفتن و نشت اطلاعات پرداخته‌اند. در این مقاله، یک مدل جدید به نام مدل پیاده‌روی نمودار وزنی تطبیقی [1] (AGW) برای تشخیص داده‌های تبدیل شده پیشنهاد شده‌است. در این مدل تمامی اسناد به صورت گراف نمایش داده می‌شوند.

در [۱۴] نویسندگان تأثیر به اشتراک‌گذاری دانش امنیت سایبری در دنیای مجازی را بررسی کردند و تأثیر آن بر کاهش ریسک امنیتی را نشان دادند. آن‌ها همچنین تمایل اندک همکاران در به اشتراک‌گذاری دانش امنیت سایبری را متذکر شدند. از جمله موانع به اشتراک‌گذاری دانش امنیتی می‌توان به از دست دادن شغل، ناآشنایی با موضوع، نگرش و بی‌اعتمادی فردی اشاره کرد. انگیزه موضوعی است که باعث می‌شود که فرد رفتاری را انجام دهد. به‌دست آوردن شهرت یا ارتقا، از جمله عوامل خارجی، و کنجکاوی از جمله عوامل داخلی برای افزایش انگیزه افراد برای اشتراک دانش امنیتی است. بنابراین سازمان‌ها باید یک محیط مناسبی برای توسعه فرهنگ اشتراک‌گذاری دانش امنیت سایبری فراهم آوردند.

در [۱۵] نویسندگان به بررسی حملات مهندسی اجتماعی پیشرفته پرداختند و نشان دادند که افراد آسیب‌پذیرترین نقطه هر سازمان از نظر امنیتی هستند. در [۱۶] نویسندگان به بررسی هوش تهدیداتی در عصر حملات سایبری پیشرفته پرداختند. آن‌ها بیان کردند که سازمان‌ها برای آنکه بتوانند جلوی حملات را بگیرند باید اطلاعات حملات پیشین را جمع‌آوری کنند. همچنین نشان دادند که نمایش استاندارد اطلاعات تهدید به ایجاد هوش تهدیداتی کمک می‌کند.

در [۱۷] نویسندگان جنبه‌های انسانی پرسش‌نامه امنیت اطلاعات را هدف قرار دادند. آن‌ها پرسش‌نامه امنیت اطلاعات را بین ۱۱۲ دانشجو تقسیم کردند و آن‌ها را در آزمایشگاه فیشینگ به کار گرفتند. نتایج بررسی‌ها نشان داد که افرادی که نمرات بالاتری را در پرسش‌نامه تعیین کرده بودند، کارایی بهتری را در آزمایشگاه فیشینگ داشتند. این به این معناست که پرسش‌نامه امنیت اطلاعات می‌تواند جنبه‌ای از امنیت اطلاعات را پیش‌بینی کند.

در [۱۸] نویسندگان به ارائه الگویی برای ارزیابی قدرت سایبری پرداخته‌اند. نویسندگان در این مقاله از روش‌های تحلیل آماری استفاده کرده‌اند و از داده‌های تجربی برای الگوسازی استفاده کرده‌اند.

در [۱۹] نویسندگان به بررسی پیش‌بینی‌کنندگان قدرت سایبری پرداخته‌اند. ایده این مقاله آن است که با شناسایی عواملی که بیشترین اهمیت را در پیش‌بینی افزایش قدرت سایبری دارند، محققان آینده ابزارهایی برای ایجاد

[1] Adaptive weighted Graph Walk

یک معیار پیچیده برای رتبه‌بندی توسعه سایبری پیش‌بینی‌شده در اختیار دارند و سیاست‌گذاران می‌توانند از اطلاعات برای توسعه راهبرد برای بهینه‌سازی کارایی در حوزه امنیت ملّی استفاده کنند.

در پژوهشی که اخیراً انجام شد [۲۰] روشی برای ارزیابی مخاطرات امنیتی سیستم‌های سایبر- فیزیکی [1] با استفاده از نظریه بازی‌ها با اطلاعات ناقص ارائه کردیم. در این روش، تقابل بین مهاجم و سیستم به‌صورت یک بازی دو نفره با اطلاعات ناقص بازیکنان مدل‌سازی شد. در مقایسه با کارهای پیشین، در این تحقیق قصد داریم به قدرت سایبری از دیدگاه متفاوتی نگاه کنیم. هدف اصلی، ارائه مدل مفهومی برای قدرت سایبری است. جنبه متمایز پژوهش انجام شده نسبت به پژوهش‌های گذشته، شناسایی و معرفی ابعاد و مؤلفه‌های جدید و مهم برای قدرت سایبری است. استفاده از این ابعاد و مؤلفه‌های این مدل مفهومی به‌منظور دستیابی به الگویی برای قدرت سایبری بسیار ضروری خواهد بود.

تعاریف و مفاهیم مبنایی

قدرت: محققان تعاریف زیادی از قدرت ارائه اده‌اند [۳; ۴]: ارگاناسکی قدرت را توانایی یک نهاد (معمولاً یک دولت) تعریف می‌کند تا رفتار نهادهای دیگر را با توجه به اهدافش تحت تأثیر قرار دهد. جوزف نای قدرت توانایی تأثیر روی دیگران برای کسب نتایج دلخواه و توانایی اجبار به انجام دادن کاری به وسیله دیگران است؛ کاری که آن‌ها، در صورت اعمال نشدن قدرت، آن را انجام نمی‌دادند.

قدرت به دو بخش سخت و نرم تقسیم می‌شود [۱; ۴]: قدرت سخت عبارت است از توانایی یک نهاد برای استفاده از تهدیدها یا جوایز برای اجبار دیگر نهادهاست به طوری‌که در غیر این صورت آن کار را انجام نمی‌دادند. در حقیقت در اینجا، موضوع اجبار مطرح است. قدرت نرم عبارت است از توانایی کسب اهداف از خلال جذب دیگران به جای اجبار. قدرت نیاز به منابع دارد. نالت قدرت ملّی را توانایی کنترل منابع، عمدتاً منابع نظامی می‌داند [۵]. منابع دیگر عبارتند از ثروت، زمان، سرمایه سیاسی، اندازه جغرافیایی، جمعیت و قدرت اقتصادی. قدرت ملّی به پنج رده – قدرت‌های کوچک، قدرت‌های میانه، قدرت‌های منطقه‌ای، قدرت‌های بزرگ و ابرقدرت‌ها – تقسیم‌بندی می‌شود. همه ملل جهان را در یک سلسله‌مراتب پویا قرار می‌گیرند که در آن به‌طور مداوم برای قدرت در ابعاد و حوزه‌های گوناگون تلاش می‌کنند [۴].

فضای سایبری: اصطلاح فضای سایبری را برای اولین‌بار ویلیام گیبسون در سال ۱۹۸۴ در رمانش به‌کار برد [۳]. فضایی که برای بقا، رشد و توسعه نیاز به مؤلفه‌های دنیای فیزیکی دارد [۱]. این مؤلفه‌ها شامل سخت‌افزار، نرم‌افزار، داده‌ها و افراد است که همه آن‌ها نیاز به منابع دیگری مانند برق، ساختمان و مخابرات دارند. به عبارت دیگر، فضای سایبر از منابع پنج حوزه مختلف از جمله زمین، دریا، هوا، فضا و فضای مجازی ساخته شده است و همچنین از آن‌ها استفاده می‌کند. فضای سایبری در برخی از جنبه‌های کلیدی منحصربه‌فرد است. فضای مجازی یک دامنه مجازی است اما این امر می‌تواند جهان را سریع‌تر و فراگیرتر از هر دامنه دیگری تحت تأثیر قرار دهد. فضای سایبری برای اهداف دیپلماتیک و اطلاعاتی بسیار مؤثر است. فناوری‌های اینترنتی موجب اشتیاق عمومی برای اخبار فوری شده است و دولت‌ها برای انجام دیپلماسی دیجیتالی تلاش می‌کنند.

در مدل سطح بالای فضای سایبری، لایه‌های مختلف به لایه‌های کاربران، محتوا، خدمات و زیرساخت تقسیم‌بندی می‌شوند در حالی که امنیت سایبری و دستورالعمل‌ها و قوانین به‌طور عمودی همه لایه‌ها را پوشش می‌دهد (شکل ۱). لایه‌های کاربران، محتوا و خدمات از لایه‌های بسیار بااهمیت در این حوزه هستند. فضای مجازی یک متعادل‌کننده است. دلیل اساسی این است که فضای سایبری از نظر زیرساخت و همچنین مالکیت توزیع شده است. به‌جز اینکه یک قدرت و متحدانش می‌توانند تمام فضای سایبری و تمام نقاط دسترسی آن را کنترل کنند، سایر قدرت‌ها و متحدانشان می‌توانند فضای سایبری و نقاط دسترسی خود را ایجاد کنند. این امر منجر به ایجاد چند حوزه مستقل می‌شود [۴]. فضای سایبر

[1] Cyber-Physical Systems

همچنین قادر به متعادل ساختن قدرت نظامی است. هزینه کم توسعه سلاح‌های پیشرفته سایبری و سهولت استقرار به‌طور بالقوه هر نهاد ملّی را قادر می‌سازد تا قدرت خود در فضای مجازی گسترش دهد.

به طور کلّی، نهادهای سایبری دارای سه مؤلفه هستند [۴]: ایدئولوژی، افراد و زیرساخت.

۱- **ایدئولوژی یک نهاد- سایبری یا فیزیکی**- ارزش‌ها، اهداف و رفتارهای اصلی او را تعریف می‌کند. انتظار می‌رود که نهادهای سایبری مانند هم‌تایان فیزیکی آن‌ها طیف وسیعی از ایدئولوژی‌ها را داشته باشند. ایدئولوژی‌های بسیاری از نهادهای سایبری از دنیای فیزیکی به‌دست می‌آید. با این حال ممکن که نهادهای سایبری آینده ایدئولوژی‌هایی داشته باشند که در جهان فیزیکی معادلی ندارند.

۲- **افراد:** افراد مؤلفه انسانی یک نهاد سایبری هستند. افراد از افراد مدیر و افراد اصلی و اعضایی تشکیل می‌شوند که شامل سهام‌داران، شهروندان و اعضای موقتی است [۴]. افراد مدیر: شبیه یک نهاد فیزیکی، یک نهاد سایبری باید یک مرکز فرماندهی و کنترل برای راهبری داشته باشد. این بخش می‌تواند شامل گروهی از افراد یا یک فرد باشد. با توجه به تنوع نهادهای سایبری، مدیران مختلفی هم باید وجود داشته باشند که اغلب آنها در موازات همتایان فیزیکی خود هستند. امروزه نهادهای سایبری در حال گسترش هستند و شکل راهبردی آنها باید در مقایسه با دنیای فیزیکی یکتا باشد. بعضی از نهادهای سایبری ممکن است راهبرد مشخصی نداشته باشند و اعضای آن در محتوا آزادی عمل داشته باشند. البته فضای سایبری باید به‌مرور زمان ساختارمندتر شود و استانداردهایی برای آن تبیین گردد. نیروی انسانی متشکل از سهام‌داران، شهروندان و اعضای موقتی است.

۳- **زیرساخت:** زیرساخت موردنیاز فضای سایبری به دو دسته فیزیکی و سایبری تقسیم می‌شود. مؤلفه‌های هر دو زیرساخت، مکمل یکدیگر هستند. منابع فیزیکی شامل تجهیزات، سوخت و افراد، منابع سایبری و فعالیت‌های نهاد را تقویت می‌کنند. به‌طور مشابه، منابع سایبری نیز باید برای پشتیبانی از منابع فیزیکی مورد استفاده قرار گیرند.

۴- **زیرساخت فیزیکی:** شامل سخت‌افزارها، نرم‌افزارها، داده‌ها و شبکه. این زیرساخت همچنین شامل مؤلفه‌هایی است که برای پشتیبانی از نیروی انسانی مورد استفاده قرار می‌گیرند مانند فضای کار، خوردن و آشامیدن. به‌منظور پایداری یک نهاد سایبری، زیرساخت فیزیکی باید پایدار، قابل اطمینان و امن باشد [۴].

۵- **زیرساخت سایبری:** فضای سایبری به‌صورت آگاهی ارائه شده توسط نرم‌افزاری که روی سخت‌افزار در محیط‌های شبکه شده کار می‌کند تعریف می‌شود. بنابراین زیرساخت سایبری از دارایی‌های سایبری مانند فرایندهای نرم‌افزاری، داده‌های در حرکت و بسته‌های داده جاری در زیرساخت فیزیکی تعریف می‌شود. حقیقتاً زیرساخت سایبری بدون زیرساخت فیزیکی کار نمی‌کند. در واقع امنیت، قابلیت اطمینان و پایداری زیرساخت فیزیکی برای کارکرد زیرساخت سایبری بسیار ضروری است. زیرساخت سایبری به حق حاکمیت دوگانه هم در فضای سایبری و هم در فضای فیزیکی نیازمند است. یا اینکه زیرساخت سایبری و فیزیکی تحت حاکمیت یک نهاد قرار داشته باشند و تحت حاکمیت آن نهاد عمل کنند.

۶- **قدرت سایبری:** قدرت سایبری به این صورت تعریف می‌شود: توانایی استفاده از فضای سایبری برای استفاده از مزایا و تأثیر بر همه رویدادها، در همه محیط‌های عملیاتی و میان همه ابزارهای قدرت. محیط‌های عملیاتی در این تعریف پنج حوزه مختلف قدرت شامل زمین، دریا، هوا، فضا و فضای سایبری است. همچنین، ابزارهای قدرت متناظر با چهار بعد قدرت شامل دیپلماسی، اطلاعات، نظامی و اقتصاد است. جوزف نای قدرت سایبری را به‌صورت زیر تعریف می‌کند: قدرت سایبری به منابعی وابسته است که حوزه فضای سایبری را مشخص می‌کند [۲]. نای قدرت را به‌صورت توانایی دستیابی به نتایج موردنظر تعریف می‌کند و قدرت سایبری را

به‌صورت توانایی دستیابی به نتایج موردنظر در فضای سایبری یا استفاده از ابزارها در فضای سایبر تعریف می‌کند [۲].

ویژگی‌های یک قدرت سایبری: قدرت سایبری آینده متشکل از فعّالان دولتی و غیردولتی خواهد بود. این فعّالان، سه مؤلفه اصلی یک نهاد سایبری که عبارتند از ایدئولوژی، نیروی انسانی و زیرساخت را خواهد داشت و با دنیای فیزیکی و سایبری کار خواهند کرد [۳; ۴]. آن‌ها چهار ویژگی مهم خواهند داشت: ۱) بقاپذیری ۲) پایداری ۳) انعطاف‌پذیری ۴) وابستگی متقابل.

۱- **بقاپذیری:** یک موجویت سایبری بقاپذیر است اگر بتواند باشد و کار کند. این موضوع شامل جنبه‌های مربوط به مؤلفه‌های یک نهاد سایبری و چهار بعد قدرت می‌شود. در واقع هر نهاد سایبری باید از نظر مؤلفه‌های یک قدرت سایبری و اعمال نفوذ بر چهار بعد قدرت، بقاپذیر باشد. برای اینکه یک نهاد سایبری بقاپذیر باشد، هر سه مؤلفه از قدرت سایبری شامل ایدئولوژی، افراد و زیرساخت باید با توجه به تغییرات محیط تغییر کند. ایدئولوژی نباید ایستا باشد و باید در حال توسعه باشد. این موضوع باعث می‌شود نهاد به اهداف بلندمدت خود دست یابد و زیرساختی پایدار و افرادی پرجنب‌وجوش داشته باشد.

به‌طور مشابه نیروهای انسانی هم باید به‌روز شوند و رشد کنند. بخش مدیریت یک نهاد سایبری باید مطمئن باشد، ایدئولوژی‌ها و مأموریت‌ها به‌روز باشند. ساختار مدیریت باید با محیط و خواسته‌های افراد عضو تطابق داشته باشد. ایده‌ها باید به‌روز شوند افراد عضو، افراد و مدیران باید به‌روز شوند تا تعهد به ایدئولوژی‌ها مشخص شود و اهداف و مأموریت‌ها پیشرفت کنند. اختلافات اعتقادی معمولاً گروه‌های مذهبی مختلفی را ایجاد می‌کند. این گروه‌ها هرچند کوچک هستند ولی منسجم هستند و ایدئولوژی روشنی دارند. بعضی از آن‌ها به سرعت رشد می‌کنند و بزرگ می‌شوند. مدل‌های مشابه گروه‌های تروریستی و مجرمانه است.

مشابه ایدئولوژی و نیروی انسانی، زیرساخت فیزیکی و سایبری هم باید با تغییر شرایط اقتصادی، سیاسی و اجتماعی به‌روز شود. معمولاً نهادهای سایبری غیردولتی از زیرساخت ارائه شده توسط نهادهای دولتی استفاده می‌کنند. اما در مورد گروه‌های تروریستی قضیه فرق می‌کند. آن‌ها باید یا از یک نهاد دولتی پشتیبانی کنند یا از اینترنت زیرزمینی استفاده کنند. برای بقا و پایداری باید روابط متعددی با نهادهای دیگر داشته باشند تا در صورت قطع یکی ازآنها عملکردشان با اختلال مواجه نشود. اما دسترسی به زیرساخت سایبری ساده است. حتی گروه‌های تروریستی هم حضور قابل‌توجهی دارند. بعضی از گروه‌های تروریستی تمایل دارند از زیرساخت فضای سایبری قرار گرفته در ایالت متحده استفاده کنند؛ زیرا سطح محرمانگی و قابلیت اطمینان زیادی ارائه می‌کند.

شکل ۱. مدل سطح بالای فضای سایبری [۳].

۲- **پایداری**: وجود پیوسته یک نهاد ویژگی مهم دیگر یک قدرت سایبری است. در دنیای فیزیکی پاک کردن ردپای هر نهادی بسیار مشکل است. به هر شکل، در فضای سایبری اینکه هر نهاد ذاتاً گذاراست، پایداری‌اش

مورد سؤال قرار دارد. یک حمله منع سرویس سایبری می‌تواند از فعالیت یک نهاد سایبری جلوگیری کند. زیرساخت سایبری یک نهاد سایبری می‌تواند منابعی باشند که تصرف شده‌اند. زیرساخت فیزیکی ممکن است قطع شده باشد و بدتر از همه اینکه همه ردپای نرم‌افزار و داده‌های نهاد ممکن است پاک شود؛ بنابراین دو جنبه از پایداری وجود دارد: اولین جنبه که نیازمندی ضعیف‌تری است آن است که یک قدرت سایبری باید بتواند در یک سطح مناسب برای تحقق دستور کار خود فعالیت کند. جنبه دوم که اساس پایداری است این است که نرم‌افزار و اطلاعاتی که پایه و اساس یک نهاد سایبری است باید پایدار باشند. بنابراین، در زمان مشکل، یک نهاد سایبری می‌تواند اجرای کدهای خود را متوقف سازد و وقتی شرایط بهتر شد دوباره از سر گیرد.

نخستین جنبه پایداری با حصول اطمینان از کارکرد زیرساخت‌های فیزیکی و سایبری حاصل می‌شود. برای این کار، زیرساخت‌ها باید موجود باشند و منابع باید پایدار و کافی باشند. نقاط دسترسی بین دنیای فیزیکی و سایبری نیز باید در دسترس باشند. به‌طور کلی، همه محیط باید برای قدرت سایبری برای حفظ ایدئولوژی و سیاست‌های خود، در کنار چهار بعد دیگر قدرت، مساعد باشد.

دستیابی به سطح اول پایداری نیازمند آن است که قدرت سایبری اتحاد و ارتباط کسب‌وکار و تجاری خود را با قدرت‌های دیگر حفظ کند. این اتحاد منجر به محافظت، ثبات و پناهگاهی امن خواهد شد. اتحاد از جدا شدن و غیرفعال شدن یک قدرت سایبری جلوگیری می‌کند. تجارت و کسب‌وکار موجب کسب درآمد و منابع می‌شوند. یک زیرساخت ابری که در میان چندین نهاد جغرافیای سیاسی گسترده شده است زمینه امنی را برای عملکرد، منابع، نقاط دسترسی می‌شود و محیط جامعی را برای اعمال قدرت و نفوذ فراهم می‌آورد.

محافظت برای دستیابی به پایداری ضروری است. محافظت باید به همه مؤلفه‌های یک نهاد سایبری، ایدئولوژی، افراد و زیرساخت اعمال گردد. این محافظت هم می‌تواند توسط خود نهاد و هم توسط قدرت‌های دیگر به دلیل وجود اتحاد اعمال گردد. دارایی‌های فضای سایبری باید توسط ابزارهای فناوری مانند رمزگذاری، مبهم‌سازی، تکرار، توزیع، سیار بودن و مخفی‌سازی مورد محافظت قرار گیرند. تکرار و توزیع دارایی‌های سیار منجر به استمرار کسب‌وکار می‌شود.

جنبه دوم، پایداری داده‌ها و نرم‌افزارهای نهاد سایبری است که برای بقای پیوسته آن نهاد ضروری هستند. اطمینان از اینکه همه نسخه‌های داده‌ها و کدها به‌طور کامل و تصادفی یا عمدی پاک نشده‌اند بسیار اهمیت دارد. رایانش ابری ضمانتی از افزونگی نیز فراهم می‌کند.

۳- **انعطاف‌پذیری**: فضای مجازی یک دامنه بسیار پویا و ناپایدار است. قطع و وصل شدن برق می‌تواند زیرساخت را قطع کند. بلایای طبیعی، حوادث، خطاهای انسانی و اعمال مخرب می‌تواند بخش‌هایی از زیرساخت را غیرفعال سازد. ریسک نبودکارکرد می‌تواند با پیچیدگی، وابستگی به فناوری، تهدیدات و خطاهای بی‌شمار و عوامل انسانی غیرمستقیم افزایش پیدا کند. انعطاف‌پذیری به‌صورت توانایی یک سیستم برای مقاومت، جذب، بازیابی یا تطابق موفقیت‌آمیز با تغییرات در محیط یا شرایط تعریف می‌شود. واضح است که انعطاف‌پذیری یک ویژگی ضروری از قدرت سایبری است. برای اینکه یک قدرت سایبری به انعطاف‌پذیری برسد، هریک از مؤلفه‌های تشکیل‌دهنده آن باید انعطاف‌پذیر باشد. بنابراین، ایدئولوژی، زیرساخت‌های سیاسی و فیزیکی و سایبری باید در برابر اختلال مقاوم باشد و در صورت وقوع اختلال باید از اختلال رهایی یابد. علاوه بر این، با توجه به نقش حیاتی اقتصاد سایبری در بقای قدرت سایبری، مهم است که آن نیز انعطاف پذیر باشد.

ایدئولوژی نفس یک قدرت سایبری است و باید اساس قانونی داشته باشد. ایدئولوژی انعطاف‌پذیر باید فوری، اما انعطاف‌پذیر، سازگار با محیط‌های فیزیکی، سایبری و انسانی باشد. همین امر در مورد یک جنبش سیاسی انعطاف‌پذیر که شامل حاکمیت و افراد عضو است برقرار است. جنبه‌های کلیدی مربوط به دولت باید به‌صورت دوره‌ای از لحاظ اثربخشی و سازگاری از طریق ذی‌نفعان اصلی ارزیابی شود. افراد عضو باید یکپارچه و متعهد به ایدئولوژی و حکومت باشند. عضویت نباید ایستا باشد. باید یک فرهنگ پرورش‌دهنده که به‌طور مداوم تجدید و نوسازی می‌کند، وجود داشته

باشد. چنین فرهنگی می‌تواند عضویت را برای زنده ماندن در حوادث طبیعی، سازگاری با تغییرات پیش‌بینی‌نشده و بازسازی نهادهای سایبری امکان‌پذیر سازد. زیرساخت‌های فیزیکی و سایبری باید انعطاف‌پذیر طراحی شود. این موضوع شامل چندین جنبه از جمله افزونگی، پشتیبان‌گیری و انعطاف‌پذیری می‌شود. علاوه بر این، اتصال سست [1] (که در آن شکست در یک گره به گره‌های دیگر نفوذ نمی‌کند) باید به‌منظور به‌حداقل‌رساندن نقاط تک‌نقطه‌ای از شکست در نظر گرفته شود.

۴- **وابستگی متقابل**: ارتباط متقابل بین نهادهای سایبری با یکدیگر چه دولتی و چه غیردولتی، ویژگی است که به نهادهای دنیای واقعی این امکان را می‌دهد که سلسله‌مراتب قدرت را تحمل کنند. این موضوع برای ارتباطات سیاسی، نظامی و دیپلماسی بسیار ضروری است. ماهیت توزیع شده فضای سایبری و این واقعیت که نهادها بسیار به یکدیگر وابسته هستند، ویژگی بسیار مهم معادله قدرت در دنیای مجازی است. وابستگی متقابل اقتصادی هم در دنیای واقعی و هم در دنیای سایبری آشکار است. در اقتصاد سایبری نهادهای سایبری تولیدکنندگان و مصرف‌کنندگان به‌هم متصل هستند که با یکدیگر در حوزه‌های اقتصادی تعامل دارند. از آنجایی که هر نهاد به دو بخش سایبری و فیزیکی وابسته هستند ارتباط بسیاری بین اقتصاد دنیای فیزیکی و سایبری وجود دارد. وجود ردپای بزرگ در دنیای سایبری نیازمند اقتصاد سایبری قوی است. همچنین نهادهای سایبری کوچک به نهادهای سایبری بزرگ وابسته هستند و این وابستگی از نظر اقتصادی برای دو طرف مطرح است.

تفاوت قدرت سایبری با قدرت در سایر حوزه‌ها

موارد زیر را می‌توان به‌عنوان تفاوت قدرت در حوزه سایبری با سایر حوزه‌ها بیان کرد [۴-۲; ۲۱]:

حوزه سایبری تنها حوزه‌ای است که به‌طور کامل ساخته دست انسان است؛ بنابراین انسان قدرت تأثیر بیشتری در آن دارد.

موانع و هزینه‌های ورود به آن کم است.

فضای مجازی گمنامی بیشتری را نسبت به سایر حوزه‌های قدرت برای کاربران ممکن می‌سازد.

حرکت و جنبش در فضای مجازی سریع‌تر و ارزان‌تر از هر حوزه دیگری است.

آسیب‌پذیری‌های نامتقارن در فضای مجازی به اعضای سایبری کوچک‌تر امکان برتری نسبت به نهادهای سایبری بزرگ‌تر می‌دهد.

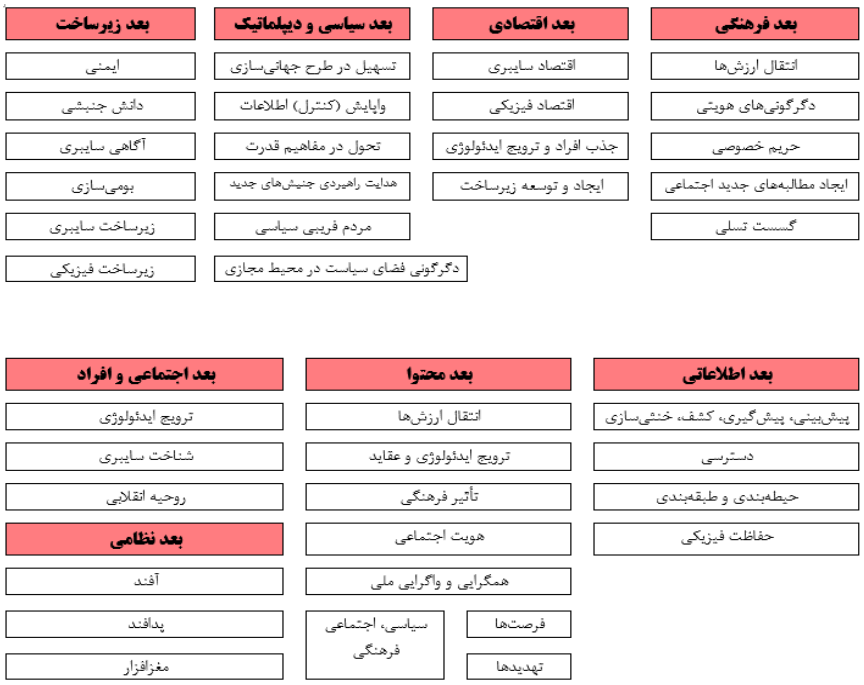
مدل قدرت سایبری: ابعاد کلان و مؤلفه‌ها

در این بخش به ارائه مدل مفهومی برای قدرت سایبری می‌پردازیم. جنبه متمایز این پژوهش، معرفی ابعاد و مؤلفه‌های جدید در مدل قدرت سایبری است که بسیار بااهمیت هستند و نباید نادیده گرفته شوند. همان‌طور که گفته شد برای چهار حوزه قدرت (زمین، هوا، دریا و فضا) چهار بعد قدرت (دیپلماتیک، اطلاعاتی، نظامی و اقتصادی) مطرح هستند [۱]. این ابعاد که در حقیقت پیش از این در زمینه نهادهای فیزیکی مورد بحث قرار گرفته‌اند در مورد قدرت‌های سایبری نیز کاربرد دارند. به دلیل وجوه متمایز قدرت سایبری از سایر حوزه‌های قدرت، ابعاد دیگری برای آن مطرح می‌گردد که در ادامه به توضیح هریک از ابعاد و مؤلفه‌های آن‌ها می‌پردازیم. ابعاد و مؤلفه‌های قدرت سایبری در شکل ۲ نمایش داده شده است.

[1] Loosly coupled

بعد فرهنگی

- **انتقال ارزش‌ها:** ارزش اجتماعی واقعیت‌ها و اموری را شامل می‌شوند که مطلوبیت دارند و مورد خواست و آرزوی اکثریت افراد جامعه هستند [۲۲]. ارزش اجتماعی، انگیزه گرایش‌های اجتماعی می‌شود و گرایش‌های اجتماعی تمایلاتی کلّی هستند که در فرد به‌وجود می‌آیند و ادراکات، عواطف و افعال او را در جهت‌های معینی به جریان می‌اندازند. این گرایش برحسب شخصیت افراد متفاوت است و به‌صورت شخصیت‌های قدرت‌گرا، دانش‌گرا احترام‌گرا و مذهب‌گرا تجلّی می‌کند. پایبندی به ارزش‌ها، میراث اجتماعی جامعه را ابقا واحیا می‌کند و ارزش‌های پایدار آن را به نسل‌های آینده انتقال می‌دهد.
- **دگرگونی‌های هویتی:** پنهان ماندن هویت‌ها در شبکه، موجب کسب هویت‌های جدید و ایفای نقش‌های اجتماعی مجازی در شبکه به وسیله افراد می‌شود. با وجود امکانات چند رسانه‌ای موجود در فضای مجازی، هنوز هم قسمت عمده‌ای از ارتباط‌ها در فضای مجازی را ارتباطات متنی در قالب رایانامه و گپ (چت) تشکیل می‌دهد. ارتباط‌های متنی می‌تواند شکل جدیدی از هویت مجازی را شکل دهد. افراد در فضای مجازی، به دلیل نبود راهنماهای چهره‌ای، می‌توانند بازنمایی‌های متفاوتی از خود ارائه دهند. در ارتباط‌های مجازی، فرد می‌تواند دیوارها را بشکند، به حوزه خصوصی دیگران وارد شود و حرف‌هایی را که حاضر نیستند در ارتباط چهره به چهره بگویند، بشنود.
- **حریم خصوصی:** با اندکی جست‌وجو در وب‌گاه‌های اینترنتی و به‌ویژه شبکه‌های اجتماعی می‌توان با تصاویر خصوصی برخی افراد و کاربران اینترنتی مواجه شود که به‌راحتی در دسترس عموم کاربران قرار گرفته است. تصاویر شخصی و خانوادگی افراد به یک‌باره از درون آلبوم‌های سنتی و پوشهٔ رایانه‌های خانگی وارد عرصه بی‌حد و مرز شبکه‌های اجتماعی شده است، اما این بار، این خود افراد هستند که تصاویر خصوصی خود را منتشر می‌کنند. این قبیل تابوشکنی، به‌تدریج بحران و تنش‌های خانوادگی و اجتماعی را دربر خواهد گرفت و بر روحیه جوانان و زوال اخلاقی ایشان تأثیرات مخرب بر جای خواهد گذاشت.



شکل ۲. مدل، ابعاد و مؤلفه‌های قدرت سایبری.

- **ایجاد مطالبه‌های جدید اجتماعی**: ایجاد سهولت در برقراری ارتباط با شهروندان سایر جوامع و آگاهی از وضعیت رفاه و معیشت آنان موجب مقایسه فرد با دیگری می‌گردد. این حقیقت، به‌ویژه در مورد جوانان و قشر فعال جامعه نمایان‌تر می‌باشد؛ زیرا جوان، سرشار از انرژی و نشاط است و همواره درصدد ایجاد تغییر در فضای خصوصی و اجتماعی خود می‌باشد. از طرفی، مسائل احساسی و روانی، از جمله تعلق خاطر کمتر به داشته‌های فرهنگی و اجتماعی خود و اعتماد به نفس کمتر، در میان این قشر از جامعه بیشتر ملموس بوده و اندک مواجهه با مظاهر رفاه اجتماعی در سایر نقاط دنیا، درخواست آنان برای تغییر سطح طبقه‌ای را افزایش داده و همین امر به ایجاد مطالبه‌های جدید اجتماعی می‌انجامد. این درخواست برای ارتقای سطح رفاه، اگرچه به‌خودی‌خود مذموم نیست و از ارزش‌های ماهوی نیز برخوردار است اما بدون هدایت و راهبری صحیح و پیگیری مطالبه‌ها از مجاری منطقی، قادر است جوامع را دچار بحران‌های اجتماعی گرداند.
- **گسست نسلی**: اکنون به دلیل دسترسی کاربران به حجم انبوهی از اطلاعات در فضای مجازی و ارتقای سطح آگاهی‌ها، نه‌تنها شکاف میان نسل اول و دوم، بلکه شکاف میان نسل دوم و سوم نیز آشکار شده است و هیچ‌یک، زبان دیگری را به‌خوبی درک نمی‌کنند. تغییر ماهیت، کمیت و کیفیت گذران اوقات فراغت، یکی از مؤلفه‌های تعیین‌کننده «سطح رفاه» و «نظام ارزشی» هر جامعه است و امروزه با گسترش فضای مجازی، این عرصه اجتماعی و فرهنگی نیز دستخوش تحول گردیده است. اگر تا پیش از این، مفهوم گذران اوقات فراغت به حضور در بوستان‌ها، سرکشی به اقوام، رفتن به سینما و نظایر آن، که به‌طور کامل یا بخش عمده‌ای از آن مبتنی بر حضور فیزیکی و ارتباط چهره به چهره بود، امروزه بخش قابل‌توجهی از این‌گونه ارتباط، جای خود را به گفت‌وگو در فضای پیام‌رسان‌ها داده است و با گسترش روزافزون فضای مجازی، سهم این ارتباط افزوده خواهد شد.

بعد اقتصادی

در حالی‌که تمام ابعاد باارزش هستند، قدرت اقتصادی (یا حداقل حمایت اقتصادی توسط قدرت‌های دیگر) ممکن است به‌عنوان مهم‌ترین بعد یک قدرت سایبری در نظر گرفته شود [۳]. بدون منابع مالی، یک قدرت سایبری نمی‌تواند ایدئولوژی خود را دنبال کند، افرادی را جذب کند و یا زیرساختی را ایجاد کند. منابع مالی همچنین برای انجام فعالیت-هایی مفید هستند که به رشد و پایداری قدرت سایبری کمک می‌کند، ازجمله فعالیت‌های انجام شده در ابعاد دیگر مانند دیپلماتیک، اطلاعاتی و نظامی.

همان‌طور که گفته شد اقتصاد دنیای واقعی و اقتصاد سایبری باید به‌هم متصل باشند. این به این علت است که فضای سایبری برای کارکردن، به منابع از دنیای واقعی نیاز دارد. تعاملات قوی بین دو اقتصاد برای بقا و پایداری یک قدرت سایبری حیاتی است [۳]. بدیهی است، شرکت‌ها و سازمان‌های جنایتکار سایبری، همانند همتایان دنیای واقعی خود، به دنبال سود باشند. سایر نهادها، از قبیل سازمان‌های تروریستی و گروه‌های اجتماعی، مذهبی و فعال، فضای سایبری را برای ترویج ایدئولوژی‌ها و فعالیت‌های خود و همچنین ایجاد درآمد استفاده می‌کنند. این سازمان‌ها اساساً سودآور نیستند. با این حال، با توجه به ماهیت عجیب فضای مجازی، قابل تصور است که برخی از آنها برنامه‌های ایدئولوژیک خود را تقویت کنند و رشد کنند تا به ساختارهای سودآوری تبدیل شوند [۱]. این مفهوم برای دولت‌های سایبری نیز برقرار است. یک نهاد سایبری می‌تواند با افراد مختلف در سراسر جهان وارد قراردادهای اجتماعی شود و خدماتی را برای آن‌ها فراهم کند و درنتیجه از شهروندان پشتیبانی پنهان و آشکار دریافت کند.

اقتصاد سایبری، امکان مبادله ارز سایبری و اعتبارات را برای کالاها و خدمات سایبری فراهم می‌کند. اقتصاد سایبری باید در موازات اقتصاد جهان واقعی باشد. با این حال، برای بقای اقتصاد سایبری، باید مکانیسم‌هایی برای تبدیل پول و اعتبارات سایبری، کالاها و خدمات سایبری به همتایان در اقتصاد فیزیکی وجود داشته باشد. دنیای سایبری برای بقا نیاز به مؤلفه‌های دنیای واقعی دارد. بنابراین، نه‌تنها باید دو اقتصاد وجود داشته باشد بلکه آن‌ها نیز باید به‌هم متصل باشند. هرچه این پیوند قوی‌تر باشد اقتصاد سایبری دوام بیشتری دارد [۳; ۴].

دو مشکل اصلی در بعد اقتصاد قدرت سایبری آن است که کاربران می‌توانند گمنام باشند و اعتبارسنجی معاملات دشوار است [۳]. یک اقتصاد سایبری قانونی نمی‌تواند رشد پیدا کند مگر اینکه خریداران و فروشندگان بتوانند به یکدیگر یا به یک واسط اعتماد کنند. مشتریان نگران حفظ حریم خصوصی اطلاعات مربوط به معاملات سایبری هستند، در حالی که تولیدکنندگان نگران اعتبار اثبات‌پذیری معاملات هستند. آینده اقتصادهای سایبری قانونی و در واقع نهادهای سایبری، به‌شدت به طراحی و اجرای فناوری‌ها و پروتکل‌هایی وابسته است که امکان معاملات اقتصادی قابل‌اعتماد بین تولیدکنندگان و مصرف‌کنندگان را فراهم می‌کنند.

بعد سیاسی و دیپلماتیک

بعد دیپلماتیک برای بقای یک قدرت سایبری ضروری هستند. هیچ نهادی در دنیای واقعی بدون روابط قوی با نهادهای دیگر نمی‌تواند کار کند. به همین ترتیب، قدرت سایبری، هرچند اندک باشد، باید ارتباطات خود را با سایر قدرت‌ها، واقعی و مجازی، برای درآمد، منابع و پشتیبانی دیپلماتیک، در واقع برای وجود خود حفظ کند. روابط دیپلماتیک بین دولت‌های سایبری همکاری‌های تجاری را افزایش می‌دهد، کمک به ایجاد زیرساخت‌ها، توسعه اقتصادی و پایداری در بحران‌های مالی می‌شود [۳].

در این بعد، نقش‌آفرینی‌های مهم فضای مجازی در ابعادی مانند تضعیف حکومت‌های سنتی، کاهش نقش مرزهای سیاسی و جغرافیایی سنتی، تحول در چگونگی مشارکت سیاسی افراد و گروه‌ها و اشاعه اطلاعات سیاسی مورد دقت قرار می‌گیرد [۲۲].

تسهیل در طرح جهانی‌سازی: ابتدا، تمایزبخشی میان اصطلاح «جهانی شدن» و «جهانی‌سازی» امری ضروری و لازم است. عموم صاحب‌نظران این عرصه، جهانی شدن را فرایندی قطعی و مفید به حال ملت‌ها و در عوض، جهانی‌سازی (از جمله جهانی‌سازی فرهنگ غرب و به‌ویژه فرهنگ آمریکایی) را طرحی با هدف تحمیل ارزش‌ها و در خدمت نظام سلطه جهانی می‌دانند. برخی از کارشناسان معتقدند روند مجازی‌سازی تمام دنیا، ادامه مسیر جهانی‌سازی است و کشورهای پیشرفته به نام هدف‌های بین‌المللی، به دنبال جهانی‌سازی از مجاری فضای مجازی هستند. آن‌ها می‌خواهند با جذابیت فضای مجازی، روند جهانی‌سازی را به کشورهای توسعه‌یافته و در حال توسعه تحمیل کنند و به شکل طبیعی، اگر راهبرد مشخص و بلندمدت برای حفظ فرهنگ ملی و بومی ملل آماج در فضای مجازی وجود نداشته باشد، به راحتی عرصه برای تحقق هدف‌های آنها فراهم خواهد شد.

واپایش (کنترل) اطلاعات: اطلاعات، منبع اصلی قدرت است. انسان به هر اندازه که از اطلاعات و آگاهی بهره‌مند باشند، به همان اندازه قادر است در عرصه‌های مختلف سیاسی، اجتماعی، فرهنگی و نظایر آن، ایفای نقش کند. صاحبان فضای مجازی، با استفاده ماهرانه از فناوری ارتباطات، امکانات وسیع و اطلاعات پالایش شده گسترده‌ای را برای به چالش کشیدن افراد غیر همراه با سیاست‌های خویش در اختیار کاربران قرار می‌دهند.

تحول در مفاهیم قدرت: قدرت، توانایی نفوذ در رفتار دیگران برای گرفتن نتیجه مطلوب است. برخلاف قدرت سخت، قدرت نرم از عناصر آشکار نفوذ و قدرت، برخوردار نیست بلکه پذیرفتنی است و در بسیاری از موارد، دلربا و برانگیزاننده است. قدرت نرم یا همان «قدرت جذاب»، مبتنی بر مزیت قدرت «نفوذ» آن است که با قانع کردن دیگران به «دوست داشتن آنچه ما دوست داریم»، هزینه‌های لازم برای قدرتمند باقی ماندن را کاهش می‌دهد. این قدرت، ناشی از جذابیت فرهنگ، آرمان‌های سیاسی و سیاست‌های یک کشور است.

هدایت و راهبری جنبش‌های جدید سیاسی ــ اجتماعی: جنبش‌های اجتماعی جدید، از مهم‌ترین جنبه‌های نرم‌افزاری تهدید امنیت ملی هر کشوری محسوب می‌گردند و حتی در خاستگاه اصلی آن یعنی ایالات متحده، جنبشی مانند «جنبش تسخیر وال استریت» توانست هشدارهای جدی به نظام سرمایه‌داری غرب دهد. عموم حاضران در این جنبش از طریق شبکه‌های اجتماعی مجازی به هم مرتبط شده و سازمان‌یافته بودند بازیگران سیاسی، از طریق رسانه‌های جدید، در بازی قدرت حضور دارند و از آنجا که اطلاعات و ارتباطات، بیشتر از طریق شبکه جهانی اینترنت، ماهواره‌ها و خبرگزاری‌ها انتشار می‌یابد، بازی سیاسی، به گونه فزاینده‌ای در فضای رسانه‌ها انجام می‌شود.

دگرگونی فضای سیاست در محیط مجازی: از دیگر کارکردهای فضای مجازی، رسانه‌ای شدن فضای سیاست می‌باشد. از دید امانوئل کاستلز، در جامعه کنونی، سیاست به معنای سیاست رسانه‌هاست. رسانه‌ها، پس‌زمینه همیشگی بازی سیاست و حوزه‌های عمومی هستند که در آن، قدرت به نمایش درمی‌آید و درباره آن داوری می‌شود

مردم‌فریبی سیاسی: حجم انبوه اطلاعات موجود در فضای مجازی، اگرچه می‌تواند عامل مهمی در ارتقای سطح دانش و آگاهی باشد اما روی دیگر سکه بیانگر این حقیقت است که افراد حاضر در این فضا، به واسطه مواجهه با این حجم از اطلاعات، کمتر از تفکر و اندیشه خود بهره می‌گیرند و گرفتار نوعی از تغافل و تجاهل (در عین بهره‌مندی ظاهری از آگاهی) می‌گردند و این موضوع از دیگر آسیب‌های جدی شبکه‌های اجتماعی مجازی است که بستر سیاسی آن، به میزان قابل‌توجهی امکان واپایش سیاسی و مردم‌فریبی را بالا می‌برد.

بعد اطلاعاتی

در واقع، ابعاد اطلاعاتی را می‌توان بسیار قدرتمند برای انجام دیپلماسی عمومی و قدرت سیاسی استفاده کرد [۳]. جاسوسی سایبری، نوعی از تهدیدات سایبری در این زمینه به شمار می‌آید. به‌طور خلاصه جاسوسی سایبری به معنی

کسب اطلاعات محرمانه از طریق به‌کارگیری توان فناوری و بدون اجازه صاحب تأسیسات رایانه‌ای است. جاسوسی سایبری می‌تواند به دلایل گوناگون یا برای رسیدن به اهداف متفاوتی انجام شود.

نکته مهمی که در تهدیدات سایبری صدق می‌کند نقش اینترنت و وجود ارتباط اینترنتی برای تحقق یافتن تهدیدها است. یعنی اگر دستگاه‌های رایانه‌ای به فضای بین‌المللی اینترنت متصل نباشند امکان تحقق تهدیدات در شکل‌های توصیف شده اگر غیرممکن نباشد به حداقل می‌رسد. به همین منظور بعضی از کشورها سعی می‌کنند به پروژه اینترنت ملّی بپردازند که خود بحث بسیار گسترده‌ای است و در کاربرد آن جای شک و تردید بسیار وجود دارد. بعضی از کارشناسان امنیت سایبری معتقدند ضرورت ندارد رایانه شما دائماً به اینترنت وصل باشد. می‌توانید با قطع اتصال اینترنت به رایانه خود امکان آسیب‌پذیری را کاهش دهید و هر وقت نیاز داشتید به اینترنت وصل شوید. طبیعی است که این نسخه می‌تواند برای رایانه‌های شخصی شفا پخش باشد ولی در دنیای امروز نمی‌توان هزاران دستگاه رایانه‌های در حال کار یک کمپانی را از اینترنت محروم کرد.

موضوع مهمی که بعد اطلاعاتی قدرت سایبری مطرح است طبقه‌بندی اطلاعات از نظر محرمانگی و محدود کردن دسترسی افراد به اطلاعات حساس است. یعنی هم اطلاعات و هم دسترسی افراد به اطلاعات طبقه‌بندی شود و به هرکس هر اندازه اطلاعات نیاز دارد دسترسی داده شود. این موضوع از آنجا در قدرت سایبری اهمیت دارد که نداشتن محدودیت دسترسی افراد به اطلاعات طبقه‌بندی‌شده و محرمانه ممکن است باعث افشای عمدی یا غیرعمدی اطلاعات برای افراد غیرمجاز (دوستان و آشنایان، در شبکه‌های اجتماعی، منزل، وسایل نقیله عمومی یا با آگاهی به دشمنان) شوند.

بعد نظامی

برخلاف ابعاد دیگر قدرت، بعد نظامی ممکن است برای بقای یک قدرت سایبری ضروری نباشد. مطمئناً، بعد نظامی برای حاکمیت و ادامه پیشرفت قدرت سایبری حیاتی است [۳]. مطمئناً قدرت‌های بزرگ و حتی منطقه‌ای باید توانایی نظامی قابل‌توجهی داشته باشند. با این حال، فعالان غیردولتی و بازیگران دولتی کوچک با دارایی محدود یا غیرنظامی می‌توانند تحت حمایت متحدان قدرتمند قرار گیرند. همان‌طور که قدرت‌های کوچک در دنیای فیزیکی نیازمند کمک قدرت‌های بزرگ برای امنیت هستند، قدرت‌های کوچک سایبری باید در برابر قدرت‌های سایبری بزرگتر محافظت شوند.

همانند دنیای فیزیکی، شرکت‌های اینترنتی و غیرقابل اعتماد نیز به قدرت‌های بزرگ دولتی برای ایمنی و امنیت متکی هستند. با این حال، شرکت‌های بزرگ به احتمال زیاد نیروهای امنیتی خود را دارند. انتظار می‌رود که کشورهای عضو سایبری تحت اختیاراتی که نهادهای غیردولتی در آن فعالیت می کنند، از این نهادها حمایت می‌کنند. با این که در دنیای واقعی، برخی از این نهادها از حامیان و نهادهای دولتی حمایت و پشتیبانی می‌کنند.

در بعد نظامی دو مؤلفه پدافند و آفند مطرح می‌شود [۴]. پدافند به مجموعه اقداماتی گفته می‌شود که در نتیجه اقدامات یک مهاجم انجام می‌شوند تا اثرات حمله را محدود کنند یا از بین ببرند. آفند به حمله پیش‌دستانه‌ای گفته می‌شود که حمله احتمالی دشمن را پیش از وقع خنثی می‌سازد.

در بعد نظامی، موضوع امنیت سایبری بسیار اهمیت پیدا می‌کند [۳; ۴]. از آنجا که یک کشور می‌تواند از طریق فضای سایبری به زیرساخت‌های حیاتی کشور دیگر حمله کند و تأثیرات مخرب سایبری یا حتی فیزیکی بر جای گذارد. بسیاری از پژوهشگران امنیت را فقدان تهدید تعریف می‌کنند و به همین اعتبار امنیت سایبری را در نبود تهدیدات عمده سایبری به سیستم‌ها میسر می‌دانند که درنتیجه آن حفاظت اطلاعات سایبری مقدورخواهد بود. امنیت سایبری مجموعه‌ای از ابزارها، سیاست‌گذاری‌ها، مفاهیم امنیتی، مقررات حفاظتی، دستورالعمل‌ها، رهیافت‌های مدیریت ریسک، آموزش بهترین شیوه‌های اجرا، فناوری‌های حفاظت از محیط و سازمان‌های سایبری و در نهایت حفاظت از سرمایه‌های کاربران است.

موضوع بسیار مهمی که در اینجا مطرح می‌شود مغزافزار است. در این جنبه از قدرت سایبری، شرایط توسط افراد متخصص بررسی می‌شوند، سپس تحلیل‌های دقیق انجام می‌گیرند و تصمیماتی اتخاذ می‌شوند که در نتیجه و دستیابی به هدف تأثیر بسیاری دارند. این تصمیمات و طراحی‌ها هم در اقدامات آفندی و هم در اقدامات پدافندی نمود پیدا می‌کند.

حملات سایبری هم راهبرد هم روش: تهدیدهای سایبری تبدیل به یک واقعیت انکارناپذیر در زندگی روزمره ما شده است. زندگی مدرن ما به دستگاه‌هایی متصل است که با هم وابستگی درونی دارند و اگر یک جای این ارتباط صدمه ببیند جای دیگری از کار می‌افتد. هر لحظه جنبه‌های گوناگون و غیرقابل تصوری از حیات روزانه ما در معرض خطر سایبری است. در این رابطه هکرهای بالقوه از دستگاه‌های بازی در یک پارک کودک گرفته تا پیچیده‌ترین دستگاه‌های بیمارستانی، زیرساخت‌های انرژی، امنیتی، و نظامی ما را هدف گرفته اند. هواپیماها یا زیر دریایی‌ها و کشتی‌ها نیز مصون نیستند.

به این اعتبار تهدید سایبری عین جنگ نظامی است و بسته به این دارد که کدام بُعد از زندگی فردی یک ملت را هدف قرار دهد [۲]. هدف از تهدید سایبری هم مانند تهدیدات نظامی ضربه زدن، ناکارآمد کردن و نهایتاً تحمیل اراده سیاسی است. بعد از شکست می‌توان دور میز مذاکره نشست و قواعد صلح را به بازنده جنگ دیکته کرد.

نتیجه مذاکرات مانند مذاکرات پس از جنگ بستگی به میزان قدرت باقیمانده برای طرف‌های مذاکره دارد. تنها تفاوت استراتژی سایبری با استراتژی نظامی در این است که جنگ سایبریی، اگرچه به صورت بالقوه می تواند موجب قتل و مرگ افراد بیگناه بشود، ولی دست کم در دوران ما به افشای اسرار سیاسی، نظامی، و اقتصادی بیشتر تمایل دارد تا به آدم‌کشی. به عبارت دیگر، جنگ سایبری می‌تواند در همه ابعاد یک جنگ کلاسیک انجام شود ولی در عین حال به شیوه‌هایی متمدنانه‌تری عمل می‌کند.

در سایه وجود امنیت سایبری [۵]:

قابلیت دسترسی برای همه کابران به تناسب نوع دسترسی تأمین خواهد شد.

صداقت، اصالت و انکار نکردن ارائه سرویس تنها در صورت وجود امنیت سایبری میسر است.

هرجا که لازم باشد اطلاعات محرمانه باید به همان صورت حفظ و در اختیار کاربران خاص خود قرار بگیرد. هرگونه تجاوز بر این اصل تجاوز بر امنیت سایبری است.

امروزه بسیاری از کشورهای جهان، قدرت لازم را برای آغاز جنگ سایبری دارند. اما هیچ توافق، مرجع یا نظامی برای کنترل یا تشخیص مشروعیت و عادلانه بودن این نوع جنگ وجود ندارد. به علاوه، همان حداقل‌های اخلاقی و عرفی درباره مشروعیت بخشیدن به جنگ نظامی متعارف در مورد جنگ سایبریی هنوز جا نیفتاده است. نویسندگان در ادامه به ابهاماتی در این حوزه اشاره می‌کنند که عبارتند از [۱۶]:

۱- **تجاوز:** طبق، تعاریف فقط جنگی عادلانه است که در برابر تجاوز یک نیروی خارجی انجام شود اما در جنگ سایبری چون تلفات انسانی در کار نیست، مفهوم تجاوز مبهم می‌شود. هم‌چنین مرز روشنی بین جاسوسی، خراب‌کاری یا مختل کردن تأسیسات وجود ندارد که همه این موارد لزوماً با واکنش نظامی روبه رو نمی‌شوند. پس چون تلفات جانی و مالی جنگ هویدا نیست، نمی‌توان تشخیص داد که متجاوز کیست و میزان تجاوز چه حدی است.

۲- **تفکیک اهداف نظامی و غیرنظامی:** طبق قوانین جنگی حمله به غیرنظامیان ممنوع است؛ هرچند در اکثر موارد این اصل رعایت نمی‌شود یا غیرنظامیان غیرمستقیم آسیب می‌بینند. اما رعایت یا تشخیص عواقب جنگ سایبری در این زمینه ساده نیست. هر حمله سایبر برای بسیاری از غیرنظامیان که به شبکه اینترنت متصلند می‌تواند پیامدهای زیانبازی داشته باشد.

۳- **تناسب:** در جنگ عادلانه قاعدتاً نباید از سلاح‌هایی استفاده کرد که میزان تخریبشان بیش از حمله‌ای است که قرار است با آن مقابله شود. اما در بیشتر موارد اگر جنگ سایبریی اتفاق بیفتد، تشخیص دامنه آسیب بسیار مشکل است و بنابراین طرف مقابل نیز می‌تواند بدون رعایت اصل تناسب در ابزارهای جنگی از هر روش گسترده‌ای در جنگ سایبریی استفاده کند. به همین دلیل، ضدحمله که در جنگ سایبریی عاملی مهم برای پیش‌گیری از حمله طرف مقابل است، از هیچ قاعده و اصل اخلاقی تبعیت نمی‌کند.

۴- **تعیین مسئولیت:** جنگ عادلانه هر طرف باید مسئولیت حملات خود را برعهده گیرد؛ اما در جنگ سایبری هر گروه، فرد یا کشوری می‌تواند چهره خود را بپوشاند و از قبول مسئولیت شانه خالی کند. پذیرش مسئولیت در جنگ فقط یک اصل اخلاقی نیست، بلکه از نظر حقوقی و جزایی نیز اهمیت دارد. بنابراین در جنگ سایبریی نیز باید مراجع و موازینی برای تشخیص هویت مسئولان حملات و جرایم وجود داشته باشد. نویسندگان به حمله استاکس نت علیه ایران اشاره می کنند و می‌گویند چون ایران نمی‌تواند عامل حمله را دقیق شناسایی کند و ضدحمله‌ای علیه او ترتیب دهد، ممکن است به اقدامات افراطی‌تر متوسل شود.

۵- **فریب‌کاری:** کنوانسیون‌های ژنو و لاهه درباره قوانین دوران جنگ، فریب‌کاری را ممنوع کرده‌اند و طرف های درگیر جنگ موظفند از روش‌های فریب‌کارانه مانند استفاده از لباس امدادرسان‌ها یا غیرنظامیان پرهیز کنند. اما در جنگ سایبری بخش زیادی از موفقیت حمله به تغییر چهره مهاجم و استفاده از پوشش‌ها و مجاری فریب‌کارانه بستگی دارد.

بعد افراد

به طور کلّی می‌توان نقش افراد در قدرت سایبری را به سه مورد تقسیم‌بندی کرد [۲]:

در مورد اول، توانایی فرد یا کشور در وادار کردن افراد به انجام کاری که مخالف با سلایق و تمایل اولیه آن‌هاست؛ برای مثال، حملات اختلال سرویس یا دستگیری وب‌سایت‌نویسان. این مورد مربوط به قدرت سخت است اما در جنبه نرم در این بعد می‌توان به تلاش فردی یا جمعی به منظور متقاعد کردن دیگران به تغییر رفتارها اشاره کرد.

در مورد دوم، فرد یا کشور مانعی را برای آزادی عمل، از طریق حذف استراتژی‌ها، ایجاد می‌کند. اگر این کار علیه مقاصد شخص باشد، جنبه قدرت سخت است، اگر این کار به‌عنوان یک موضوع قانونی نزد شخص پذیرفته شود، مصداق قدرت نرم است؛ برای مثال محدود کردن سرعت اینترنت یا فیلتر کردن. حال اگر از الگوریتم‌هایی استفاده شود که افراد را به سمت سایت‌ها یا موتورهای جستجوری خاصی هدایت کند، قدرت نرم محسوب می‌شود.

در مورد سوم، شکل دادن سلایق اولیه شخص به‌طوری که وی به مسائلی فکر می‌کند که هرگز فکر نکرده است. برای مثال ایجاد سایت‌هایی که تعداد محدودی به آن دسترسی دارند که با این کار، وی را وادار به پذیرش خطوط فکری خاصی می‌کنند.

یک فرد نقش‌های مختلفی مانند یک عضو جامعه، کاربر سیستم، مالک اطلاعاتی سیستم، یا هکر و مهاجم به اطلاعات سیستم ایفا می‌کند. افراد معمولاً نقاط اتصال سست در زنجیره امنیتی اطلاعات شناخته می‌شوند [۲۳]. آن‌ها رمزعبور و نام‌کاربری خود را با همکاران به اشتراک می‌گذارند، آن‌ها را روی برگه می‌نویسند و به صفحه نمایش می‌چسبانند یا روی میز قرار می‌دهند، ایمیل‌های ناشناخته را باز می‌کنند، از اینترنت نرم‌افزار دانلود می‌کنند، سیستم را در حالت باز و قفل نشده رها می‌کنند. بنابراین کاربران به عمد یا غیرعمد تهدید بالقوه بزرگی برای سیستم‌های سایبری هستند.

مهاجمان به طور کلی به دو دسته مهاجمان داخلی و خارجی تقسیم‌بندی می‌شوند [۲۴]. مهاجم داخلی می‌تواند اثرات مخرب‌تری را بر روی سیستم داشته باشد و این موضوع به دلیل سطح دسترسی او و داشتن مجوزهای لازم است.

یک مهاجم داخلی اطلاعات کافی درمورد سیستم را دارد و محل منابع بسیار بقرارزش سیستم را می‌شناسد و می‌داند چه زمانی و چگونه رد حمله خود را از بین ببرد.

کاربران و کارمندان سازمان‌ها و شرکت‌ها می‌توانند توانایی‌ها، دانش و تلاش خود را برای افزایش امنیت سایبری تجمیع کنند و به اشتراک بگذارند. اشتراک دانش امنیت سایبری نقش بسیار مهمی را بر افزایش دانش و آگاهی امنیتی افراد ایفا می‌کند. و دانش امنیتی افراد یکی از مهم‌ترین عامل‌های قدرت سایبری است [۲۴; ۲۵].

نصب بدافزارها به‌صورت غیرعمد، حملات مهندسی اجتماعی، و فیشینگ[1] از جمله اشتباهات کاربران در حوزه امنیت سایبری است. مهندسی اجتماعی به فعالیت‌های مخرب حاصل از تعاملات انسانی گفته می‌شود. در این روش، مهاجم از فریب دادن کاربران در جهت انجام اشتباهات امنیتی یا دادن اطلاعات حساس سوءاستفاده می‌کند. معمولاً حملات مهندسی اجتماعی در چند مرحله اتفاق می‌افتند [۲۶]. مهاجم در قدم اول فرد قربانی را زیر نظر می‌گیرد تا اطلاعات پیش‌زمینه‌ای لازم، مانند راه‌های احتمالی ورود و پروتکل‌های امنیتی ضعیف را برای ادامه حمله جمع‌آوری کند. سپس، مهاجم در راستای جلب اعتماد او گام برمی‌دارد و محرّک‌هایی را برای اقدامات بعدی برای نقض اقدامات امنیتی مانند افشای اطلاعات حساس یا اعطای دسترسی به منابع مهم ایجاد می‌کند.

حمله فیشینگ به‌عنوان یکی از محبوب‌ترین انواع حمله‌های مهندسی اجتماعی شناخته می‌شود [۲۶]. در این حمله، مهاجم با ارسال ایمیل یا پیام کوتاه قصد دارد احساس اضطرار، کنجکاوی یا ترس در فرد قربانی ایجاد کند. سپس او را ترغیب می‌کند تا اطلاعات حساس را افشا کند. روی پیوندها به وب‌سایت‌های مخرب کلیک کند یا پیوست‌هایی را که حاوی بدافزار هستند باز کند. در چنین محیط پویایی، به اشتراک‌گذاری دانش امنیتی بین همکاران نه‌تنها سطح آگاهی افراد را بالا می‌برد بلکه هزینه ارتقای امنیت سایبری سازمان را کاهش می‌دهد. به اشتراک گذاشتن تجربه‌های امنیتی گذشته بسیار می‌تواند در ارتقای امنیت سایبری مؤثر باشد. اما موضوعی که وجود دارد این است که انگیزه برای به اشتراک‌گذاری دانش امنیتی بین همکاران یک موضوع چالش‌برانگیز است.

مهاجمان خارجی از طرف دیگر ابتدا پیش از انجام حمله سطح مجوز و دسترسی‌های لازم را به‌دست بیاورند و اطلاعات خود را در مورد سیستم کامل کنند. برای یک مهاجم خارجی به‌دست آوردن اطلاعات از یک فرد داخلی بسیار کم‌هزینه‌تر و سریع‌تر از گذرکردن از لایه‌های مختلف حفاظت سیستم است. از طرفی مهاجمان داخلی زمان لازم را در اختیار دارند تا به فرصت مناسب دست یابند.

تحقیقات نشان می‌دهد که ۷۰ درصد حملات سایبری منشأ داخلی دارد حال آنکه ۹۰ درصد کنترل‌ها و نظارت‌های امنیتی بر تهدیدات و حملات خارجی متمرکز است [۲۴]. باید یک سطحی از تعادل بین سطح دسترسی موردنیاز کاربر برای انجام کارهایش و کنترل و بازرسی او برقرار شود. وفاداری، اعتماد و دانش امنیتی بسیار بااهمیت است اما تلاش‌هایی باید برای تشخیص آن‌ها برای افراد یک سازمان فراهم شود.

تحقیقات نشان داده است که تهدیدات و حملات فرد داخلی بسیار به شرکت و بخش کاری وابسته است. اغلب حملات فیزیکی و الکترونیکی توسط یک فرد داخلی آغاز می‌شود. اما بعضی از حملات تنها توسط فرد داخلی قابل انجام است. برای مثال، فاش کردن بدون مجوز اطلاعات محرمانه و خرابکاری دارایی‌هایی که تنها کارمندان به آن دسترسی دارند.

افراد داخلی ممکن است محرمانگی، جامعیت و دسترس‌پذیری اطلاعات را به‌طور عمدی یا غیرعمدی هدف قرار دهند. تحقیقات نشان داده است که وقایع امنیتی اغلب به‌طور غیرعمد اتفاق می‌افتد و اثرات آن می‌تواند حتی از حملات عمدی هم مخرب‌تر باشد. گاهی اوقات فعالیت ظاهراً بی‌ضرر یک فرد داخلی مانند دسترسی به اینترنت بی‌جا و نامناسب

[1] Fishing

نه‌تنها می‌تواند زمان و منابع یک سازمان را هدر دهد بلکه ممکن است سیستم‌ها و شبکه سازمان را در مورد تهدید ویروس‌ها و بدافزارها قرار دهد یا اعتبار و خوش‌نامی سازمان را خدشه‌دار کند.

در سال‌های اخیر شاهد رشد تهدیدات افراد داخلی هستیم [۲۴; ۲۵]:

اغلب سازمان‌ها و شرکت‌ها بیشتر نگران حملات خارجی هستند.

در سال‌های اخیر اغلب کارمندان موقتی منبع بیشترین تهدیدات بوده‌اند.

تعداد بسیاری از ویروس‌ها و بدافزارها منشأ داخلی داشته‌اند.

تعداد بسیاری از اتفاقات به دلیل استفاده غیرمجاز از سطح دسترسی و کنترل غیرمجاز بوده است.

۱۹ درصد حملات، عمدی شناخته شده‌اند.

تهدیدات افراد داخلی باید شناسایی و ارزیابی شوند و عکس‌العمل‌های مناسب آن پیش‌بینی شوند. تهدیدات افراد داخلی مانند تومور هستند اگر زود آن را شناسایی کنید مدت کوتاهی را درگیر آن خواهید بود اما شانس ترمیم بالا خواهد بود. اما اگر آن را نادیده بگیرید رشد خواهد کرد و زمان کوتاهی را به شما خواهد داد و شما را از بین خواهد برد.

مهم‌ترین کاری که در بعد افراد می‌تواند صورت گیرد افزایش سطح دانش سایبری افراد از طریق فراهم کردن آموزش‌های مناسب برای آن‌هاست.

موضوع بعدی بومی‌سازی نرم‌افزارها و برنامه‌هایی است که جنبه عمومی دارند و توسط بیشتر افراد جامعه مورد استفاده قرار می‌گیرند. کمترین مزیت این کار قابلیت پیگیری قضایی بهتر و در نتیجه امکان رعایت قوانین هرچه بیشتر توسط افراد جامعه است. به‌جز آن بسیاری از سازمان‌های دولتی امروزه کارهای حساس خود را از طریق شبکه‌های اجتماعی پیگیری می‌کنند. این موضوع می‌تواند یک رخنه اطلاعاتی ایجاد کند.

بعد محتوا

فضای سایبری، فضایی مناسب و بسیار مؤثر برای ترویج ایدئولوژی و توضیح دیدگاه‌های مختلف به طرفداران و مخالفان است. امروزه فراگیری اینترنت و فناوری‌های جدید ارتباطی- اطلاعاتی، موجب ظهور فضای مجازی در کنار جهان واقعی شده و این امر، معادله‌ها و الگوهای ارتباط‌های سنتی تولید، انتقال و مصرف اطلاعات را برهم زده و موجب تغییر در آن شده است.

چنین فضایی، به‌عنوان واقعیت مجازی یکپارچه، از ویژگی‌هایی مانند بی‌مکانی، فرازمانی، صنعتی محض بودن، محدود نبودن به قوانین دولت- ملت‌ها، قابلیت دسترسی همزمان به فضاهای فرهنگی، اعتقادی، اقتصادی، سیاسی و نیز آزادی از هویت جنسی برخوردار است [۲۷; ۲۸]. این وبگاه‌ها محیطی را فراهم آورده‌اند که کاربران، فارغ از ابعاد جغرافیایی، جمعیتی، جنسیت و ایدئولوژی‌های متفاوت، با دیگران، احساس خودی بودن، صمیمیت، امنیت و حفاظت می‌کنند و در قالب بارگذاری ویدئو، مرور ویدئوی دیگر کاربران، بار گذاشتن یادداشت و ... به فعالیت می‌پردازند.

با خلق جهان مجازی، اکنون کشورهایی در فضای مجازی وجود دارند که هرکدام شامل چندین شهر، با شهروندانی فعال و مرتبط می‌باشند، با این تفاوت که اهالی این شهرها شاید هیچ‌وقت یکدیگر را ندیده، ولی ممکن است گاه در این فضا، تشکل‌های اجتماعی یا صنفی منسجمی تشکیل داده باشند. اینترنت به‌عنوان رسانه نوظهور جهانی، در ابتدای ورود به کشور در سال ۱۳۷۰، چون از بستر اجتماعی و فرهنگی آن نشأت نگرفته بود، با نوعی بیگانگی در محیط مواجه بود و حتی پس از ورود این فناوری، دانشگاه‌ها و دانشگاهیان، فاقد علم و تخصص کافی در این زمینه بودند. از این رو، تا سال‌ها برخورد با آن، از موضع انفعال بود و پیش‌فرض اصلی مسئولان نیز بر «تهدیدآمیز» بودن این پدیده قرار داشت. با گذشت زمان و آشکار شدن ابعاد مختلف و متنوع اثرگذاری فضای مجازی و وقوف بیشتر به ماهیت دوگانه (تهدید/ فرصت) این رسانه، توجه به شناخت جنبه‌های فرصت‌زایی آن نیز بیشتر شد و افزون بر دانشگاه‌ها، مراکز دینی مانند حوزه‌های علمیه نیز وارد فعالیت در این عرصه گردیده و به تولید محصولاتی به نفع دین و فرهنگ پرداختند.

مبنا و هدف اصلی اینترنت، برداشتن فاصله جغرافیایی میان انسان‌های سراسر دنیا و ایجاد تحول در عرصه ارتباطات و تبادل اطلاعات است. در حالی که هیچ‌کس تصور نمی‌کرد روزی جنبه اجتماعی اینترنت به‌صورت کاربرد اصلی آن درآید و شبکه‌های اجتماعی اینترنتی پا به عرصه وجود بگذارد. در میان اشکال مختلف استفاده از اینترنت؛ شبکه‌های اجتماعی، به‌عنوان پدیده هزاره سوم تا الان موقعیت والاتری پیدا کرده است.

سه راه برای کنترل اینکه چه چیزی در رسانه اجتماعی مبادله می‌شود وجود دارد [۲۸]: ۱) توزیع ایده ۲) ربودن ایده و ۳) ایجاد ایده. توزیع ایده بسیار سریع رخ می‌دهد و کمترین میزان منابع را نیاز دارد. دو مورد بعدی به منابع بیشتری نیاز دارد. که معمولاً از شبکه‌های بات برای انتقال خودکار استفاده می‌شود [۲۷]. حضور افراد در شبکه‌های اجتماعی، احتمال مشارکت‌ها و کنش‌های اجتماعی را افزایش می‌دهد. هرچه پیوند افراد و اعضا در این شبکه‌ها بیشتر و انبوه‌تر باشد، امکان همراهی، تعامل، نزدیکی دیدگاه‌ها، حرکت هم‌سو و مشترک نیز افزایش خواهد یافت. در یک شبکه اجتماعی، افراد هم اهداف سیاسی و هم اهداف شخصی را پیگیری می‌کنند و در عین حال، با دیگر افراد و سازمان‌ها نیز تعاملی چندگانه دارند. ضمن اینکه، تماس‌ها و ارتباط‌های شخصی، مانند وسیله‌ای برای پیوند دادن سازمان‌ها و گروه‌ها عمل می‌کنند. سایر ویژگی‌های شبکه‌های اجتماعی مجازی عبارتند از: به اشتراک‌گذاری، بسیج‌کنندگی و سازمان‌دهی، دوستی، اعتماد، حلقه‌های مخاطبان، استناد و تعمیم، چندرسانه‌ای بودن، گپ، نقد بی‌رحمانه، دنبال کردن و دنبال شدن، شخصیت‌بخشی، بازنشر، خرد جمعی، جهانی بودن، سرگرمی، ساختار دموکراتیک، قدرت سرمایه اجتماعی، تحرک اجتماعی و ابتکار و خلاقیت.

شبکه‌های اجتماعی و تحول فرهنگی: به لحاظ تاریخی، دگرگونی فنّاورانه را که منجر به ایجاد و اختراع شاه‌راه اطلاعاتی شده است، با اختراع بزرگ حروف الفبا در یونان ۷۰۰ سال پیش از میلاد مشابه می‌داند و معتقد است برای نخستی بار در تاریخ رسانه، ابرمتن یا فرازبانی شکل گرفته است که شیوه‌های مکتوب، شفاهی، دیداری و شنیداری ارتباطات انسانی را در چارچوب نوعی نظام، یکپارچه می‌سازد [۲۷]. این پدیده که شاه‌راه اطلاعاتی دارد، به دلیل قابلیت یک‌پارچه‌سازی متن، تصویر و صدا در یک سامانه یا شبکه جهانی، ماهیت ارتباطات را دستخوش دگرگونی های بنیادین ساخته است و از آنجا که ارتباطات نقش تعیین کننده‌ای در شکل‌دهی به فرهنگ دارد، فرهنگ نیز به تبع دگرگونی‌های فنّاورانه جدید، دگرگونی‌های بنیادی دیگری را از سر می‌گذراند. در نظر کاستلز، یکی از پیامدهای مهم گسترش فنّاوری های اطلاعات و ارتباطات نوین مبتنی بر آن، دگرگونی فرهنگ‌هاست. از این رو، در اثر ایجاد و گسترش شاهراه‌های اطلاعاتی، فرهنگ نوینی در حال ظهور است.

تأثیر شبکه‌های اجتماعی بر هویت اجتماعی: در دوران معاصر، مسئله هویت بیش از هر عصر دیگری ذهن انسان امروزی را به خود مشغول کرده است [۲۷]. حضور انسان در شاهراه‌های ارتباطی و دسترسی او به امکانات جامعه اطلاعاتی هویت و هویت‌سازی‌های سنتی را با دشواری و چالش‌های عمده‌ای روبه رو کرده است. ویژگی‌های ارتباطات الکترونیکی حاکم بر شبکه‌های اجتماعی، شرایطی متفاوت از روابط حقیقی و رو در رو را برای کاربران آن فراهم می‌کند. سرعت عمل، ناشناس ماندن و سیال بودن می‌تواند فضای یکسان و مشابهی را فارغ از الزامات ساختی (جنسیتی، طبقاتی، قومی، نژادی و مکانی) فراهم سازد که مستعد تجارب متفاوتی برای کاربران آن است. تعاملات آزمایشی، کنجکاوانش یا با نیت افزایش ظرفیت شناختی، کاربران اینترنتی را با ذهنیت و گرایش جدیدی تجهیز می‌کند که می‌تواند رفتار و تعاملات آن‌ها را در دنیای حقیقی به چالش بکشاند و تغییراتی را هرچند جز ئی در میدان عمل اجتماعی آن‌ها فراهم سازد. فضای مجازی این امکان را فراهم می‌کند که افراد نیازها، خواست‌ها و بازاندیشی در هویت خویش را تا درجاتی به دنیای حقیقی خود تسریع دهند و شرایط تازه‌ای را برای گفتگو، تفاهم و تعامل در دنیای مجازی و حقیقی فراهم آورند.

تأثیر شبکه‌های اجتماعی بر همگرایی و واگرایی ملّی: تأثیر فعالیت شبکه‌های اجتماعی بر هم‌گرایی و واگرایی بین اقوام مختلف از رویکرد کلان را به شرح زیر می‌توان در نظر گرفت [۲۷]:

- **الف) رویکرد تقویت واگرایی:** طرفداران این رویکرد، مسئله یاد شده را باعث تضعیف همبستگی بین اقوام مختلف می‌دانند. آنچه از تجربه‌های موردی در فضای فیسبوک به‌دست می‌آید این است که گفتمان غالب در این عرصه، در اختیار آن دسته از فعالان قومی است که هویت قومی خود را بر هویت ملّی ترجیح می‌دهند و فعالیت‌های قوم‌مدارانه و هویت‌طلبانه آن‌ها تقویت‌کننده هویت قومی است. در برابر هویت ملّی نیز یا خنثی یا تخریب‌کننده برخورد می‌کنند.
- **ب) رویکرد تقویت همگرایی:** معتقدان به این رویکرد، تقویت هویت قومی و فعالیت‌های قومی در شبکه‌های اجتماعی را تهدیدی علیه هویت ملّی نمی‌دانند و معتقدند در صورت استفاده از فرصت‌های این فنّاوری و هدایت صحیح این فعالیت‌ها، همگرایی قومی و ملّی در کشور افزایش خواهد یافت.
- **ت) رویکرد نسبی گرایی:** معتقدان به این رویکرد، ماهیت کنش‌های افراد، دغدغه‌ها و مطالبات آن‌ها و نوع برخورد حکومت با خواسته‌های این گروه‌ها را از مهم‌ترین عوامل همگرایی و واگرایی قومی در یک کشور می‌دانند. اگر سیاست‌های اجتماعی، فرهنگی و رسانه‌ای در دنیای واقعی و واقعیات اجتماعی با خواسته‌های دنیای مجازی هم‌خوان و هم‌نوا نباشد و دنیای واقعی نتواند به پوشش حداقل این مطالبات پاسخ دهد، واگرایی ملّی افزایش می‌یابد. در جوامع چند قومی، جامعه ملّی زمانی شکل می‌گیرد که حقوق شهروندی ملاک اصلی تابعیت و هویت ملّی یک شخص قرار گیرد. در غیر این صورت، جامعه‌های متفاوت و گروه‌های قومی مختلف، هر یک در صدد واگرایی و پیگیری خواسته‌ها و مطالبات خود برمی‌آیند و به جامعه ملی فراگیر عنایتی نخواهند داشت. تنها شهروندمحوری فارغ از قومیت، مذهب و منطقه جغرافیایی می‌تواند زمینه هم‌گرایی ملّی را فراهم کند و به این ترتیب، شبکه‌های اجتماعی نیز می‌توانند به تحقق این امر کمک کنند.

بعد زیرساخت حیاتی

امروزه می‌توان زیرساخت‌های حیاتی را به‌عنوان یکی از ابعاد مهم قدرت سایبری در نظر گرفت. با ترکیب فناوری‌های ارتباطی و رایانشی با فرایندهای فیزیکی، سیستم‌های سایبر- فیزیکی (CPS)[1] ایجاد شده‌اند [۲۹]. سیستم‌های سایبر-فیزیکی، سیستم‌هایی مبتنی بر رایانه هستند که فرایندهای فیزیکی را کنترل و نظارت می‌کنند [۳۰]. این اجماع به‌منظور رسیدن به کارآمدی، قابلیت اطمینان و استحکام بیشتر سیستم‌های فیزیکی به‌کاررفته در کاربردهای مختلف است. به دلیل کاربرد این سیستم‌ها در زیرساخت‌های حیاتی مانند شبکه برق، شبکه توزیع گاز و آب، صنایع، خودروهای پیشرفته و پزشکی، امنیت این سیستم‌ها بسیار اهمیت پیدا می‌کند.

سیستم‌های سایبر- فیزیکی، یکپارچه‌سازی سیستم‌های رایانه‌ای و ارتباطی با فرایندهای فیزیکی هستند. این اجماع به‌منظور رسیدن به کارآمدی، قابلیت اطمینان و استحکام بیشتر سیستم‌های فیزیکی است، اما در عین حال، این سیستم‌ها را در معرض تهدیدات امنیتی جدیدی قرار داده است. برخلاف سیستم‌های سایبری، نفوذ به سیستم‌های سایبر-فیزیکی لزوماً به معنای خرابی آن‌ها نخواهد بود، بلکه هدف مهاجم آن است که بتواند خسارت‌ها و اختلال‌های فیزیکی به این سیستم‌ها وارد کند.

ارتباط تنگاتنگ فرایندهای فیزیکی با فناوری‌های ارتباطات و اطلاعات در این سیستم‌ها، نگرانی‌های امنیتی جدیدی را مطرح می‌کند که با روش‌های موجود قابل برطرف کردن نیستند. با فرض اینکه روش‌های جدیدی نیز با توجه به ساختار و شرایط خاص این‌گونه سیستم‌ها برای حفظ امنیت آن‌ها ایجاد شوند، نمی‌توان انتظار داشت که فنون امنیتی ارائه شده برای حفظ تمام و کمال امنیت یک سیستم سایبر- فیزیکی کافی باشند؛ چون رفتار و تفکر مهاجمان این

[1] Cyber-Physical Systems

سیستم‌ها عاملی پویاست که با وجود تمام پیش‌بینی‌ها و در نظر گرفتن تمام احتمالات ممکن، امکان بروز نمونه جدید و دیده نشده‌ای از آن وجود دارد.

آنچه امنیت سیستم‌های سایبر- فیزیکی را بسیار بااهمیت می‌کند ارتباط بسیار زیاد این سیستم‌ها با ایمنی و دارایی‌های انسان است [۳۱]. برای مثال، یک سیستم سایبر- فیزیکی که برای نظارت و کنترل سیستم‌های ریلی و حرکت قطارها مورد استفاده قرار می‌گیرد مستقیماً با جان انسان‌ها در ارتباط است و به خطر افتادن این سیستم جان انسان‌ها را به خطر می‌اندازد. یا یک سیستم کنترل صنعتی که برای کنترل و نظارت بر خطوط انتقال گاز، برق و آب استفاده می‌شود یا یک سیستم کنترل‌کننده نیروگاه اتمی نمونه‌هایی از سیستم‌های سایبر- فیزیکی هستند.

به دلیل وابستگی زیرساخت‌های حیاتی، به خطر افتادن امنیت یک سیستم، امنیت سیستم‌های دیگر را هم تهدید می‌کند. برای مثال، یک خرابی امنیتی در کارخانه تولیدکننده سوخت، که به خط لوله گاز برای تولید برق برای شبکه برق وابسته است، کارکرد شبکه برق را هم به خطر می‌اندازد [۳۱; ۳۲].

وقوع حمله سایبری که فرایندهای فیزیکی را هدف قرار داد اثبات کرد که حملات سایبری می‌توانند منجر به خسارت فیزیکی شوند. محققان دانشگاه کالیفرنیا نشان دادند که مهاجمان می‌توانند با تزریق کدهای بدخواهانه با دسترسی فیزیکی یا حتی از راه دور با استفاده از بلوتوث یا واحد تله‌ماتیک[1] کارکرد خودروها را تهدید کنند [۳۳]. بنابراین با توجه به پیوند بسیار عمیق اغلب سیستم‌های سایبر— فیزیکی با زیرساخت‌های حیاتی و در نتیجه ارتباط زیاد آن‌ها با زندگی بشر و دارایی‌های ملّی، بحث امنیت در این سیستم‌ها بسیار اهمیت دارد.

روش‌های امنیت اطلاعات به تنهایی می‌توانند امنیت ارتباطات را تضمین نمایند و برای سیستم‌هایی با فرایندهای فیزیکی کافی نیستند. در واقع روش‌های امنیت شامل احراز هویت، کنترل دسترسی و جامعیت پیام برای داده و اندازه‌گیری‌های فرایند فیزیکی کارآمد نیستند [۳۴]. به‌ویژه در مورد حملات روز صفر [۳۴] و حملات افراد خودی [۳۵] با دسترسی مجاز به کنترل فرایند، حسگرها و محرّک‌ها این موضوع بیشتر نمود پیدا می‌کند.

حملات بدخواهانه به سیستم‌های سایبر- فیزیکی ممکن است تأثیرات و خسارت‌های فیزیکی و جانی به دنبال داشته باشد [۷]. ممکن است منجر به آلودگی محیطی شوند، تجهیزات سیستم یا محصولات را هدف قرار دهند. قبل از هر اقدامی باید امنیت این سیستم‌ها مورد مطالعه و ارزیابی قرار گیرد تا بتوان در حد امکان از اثرات مخرب حملات امنیتی در این سیستم‌ها جلوگیری کرد.

نتیجه‌گیری

فضای سایبری، یک میدان نبرد جدید است که در آن بسته‌های شبکه می‌توانند تقریباً بلافاصله در سراسر جهان به سیستم‌های فیزیکی، از جمله سیستم‌های زیربنایی در حوزه‌های فیزیکی و سایبری، ارسال شوند. بدون شک، فضای مجازی تبدیل به یک حوزه اقتصادی مهم شده است [۴; ۵]. تقریباً تمام عملیات بانکداری در فضای مجازی رخ می‌دهد و در حال شکوفایی است [۵].

ابعاد قدرت سایبری را می‌توان به هفت بعد فرهنگی، اقتصادی، سیاسی و دیپلماتیک، اطلاعاتی، نظامی، اجتماعی و زیرساخت‌های حیاتی تقسیم‌بندی کرد. اگرچه این ابعاد کاملاً مجزا نیستند و می‌توانند از بعضی از جهات هم‌پوشانی داشته باشند، اما به دلیل اهمیت هریک به‌طور مستقل در نظر گرفته شده‌اند در بعد فرهنگی مسائلی از قبیل انتقال ارزش‌ها، دگرگونی‌های هویتی، حریم خصوصی، ایجاد مطالبه‌های جدید اجتماعی، گسست نسلی مطرح است که به لایه‌های کاربران و محتوای مدل فضای سایبری مربوط است. بعد اقتصادی، یکی از مهم‌ترین ابعاد قدرت سایبری در نظر گرفته می‌شود؛ زیرا تأثیر بسیار زیادی در تداوم، پایداری و پیشبرد اهداف و آرمان‌های آن دارد. این بعد بیشتر با لایه‌های

[1] Telematic

زیرساخت، خدمات در ارتباط است هرچند که تا حدودی به لایه‌های کاربران و محتوا هم مربوط می‌شود. در بعد سیاسی و دیپلماتیک موضوعاتی از قبیل تسهیل در طرح جهانی‌سازی، کنترل اطلاعات، تحول در مفاهیم قدرت، هدایت و راهنمایی بخش‌های جدید سیاسی، دگرگونی فضای سیاست در محیط مجازی، و مردم فریبی‌سیاسی مطرح می‌شود. در بعد محتوا نیز ترویج ایدئولوژی و توضیح دیدگاه‌های مختلف به مخاطبان مطرح است. در بعد نظامی مفاهیم تروریست سایبری، جنگ سایبریی و جاسوسی مطرح است. در بعد اجتماعی که یکی از مهم‌ترین ابعاد است، افراد جامعه، شناخت سایبری و روحیه دفاعی مطرح هستند. و در زیرساخت‌های حیاتی ایمنی و امنیت محیطی، فردی، اجتماعی و منابع مالی مطرح است.

قدرت سایبری و توانایی دفاع در برابر حملات به زیرساخت‌های حیاتی، نقش بسیار مهمی در برقراری امنیت ملّی دارد. از آنجا که به خطر افتادن زیرساخت‌های حیاتی موجب به خطر افتادن جان افراد و اموال ملّی خواهد شد، دستیابی و محافظت از این سطح قدرت سایبری بسیار با اهمیت است.

از طرفی یک فرد نقش‌های مختلفی مانند یک عضو جامعه، کاربر سیستم، مالک اطلاعاتی سیستم، یا هکر و مهاجم به اطلاعات سیستم ایفا می‌کند. افراد معمولاً نقاط اتصال ضعیف در زنجیره امنیتی اطلاعات شناخته می‌شوند. آن‌ها رمزعبور و نام‌کاربری خود را با همکاران به اشتراک می‌گذارند، آن‌ها را روی برگه می‌نویسند و به صفحه کلید می‌چسبانند و یا روی میز قرار می‌دهند، ایمیل‌های ناشناخته را باز می‌کنند، از اینترنت نرم‌افزار دانلود می‌کنند، سیستم را در حالت باز و قفل‌نشده رها می‌کنند. بنابراین کاربران به‌طور عمد یا غیرعمد تهدید بالقوه بزرگی برای سیستم‌های سایبری هستند. بنابراین یکی از ویژگی‌های مهم کاربران که در دستیابی به قدرت سایبری تأثیر دارد دانش سایبری است.

به‌عنوان تحقیق آینده قصد داریم الگویی را برای قدرت سایبری ارائه کنیم. به این منظور در مورد مبانی، افق و چشم انداز، اهداف و آرمان‌ها و تدابیر الگوی ارائه شده خواهیم پرداخت. هدف از ارائه این الگو تلاش در راستای حرکت به سوی تبدیل شدن به یک قدرت سایبری است.

References

[1] Kramer, F. D., Starr, S. H., & Wentz, L. K. (2009). *Cyberpower and national security*. Potomac Books. https://www.amazon.com/Cyberpower-National-Security-Franklin-Kramer/dp/1597974234

[2] Movahedi Sefat, M. R. (2007). National Security in Cyberspace, Opportunities and Threats, Strategic Defense Studies. *Strategic Defense Studies*, *8*(30), 245-276. http://ensani.ir/file/download/article/20101228093126-44.pdf

[3] Rowland, J., Rice, M., & Shenoi, S. (2014). The anatomy of a cyber power. *International Journal of Critical Infrastructure Protection*, *7*(1), 3-11. https://doi.org/10.1016/j.ijcip.2014.01.001

[4] Rowland, J., Rice, M., & Shenoi, S. (2014). Whither cyberpower? *International Journal of Critical Infrastructure Protection*, *7*(2), 124-137. https://doi.org/10.1016/j.ijcip.2014.04.001

[5] Zilincik, S., Myklin, M., & Kovanda, P. (2019). Cyber power and control: a perspective from strategic theory. *Journal of Cyber Policy*, *4*(2), 290-301. https://doi.org/10.1080/23738871.2019.1635177

[6] Mehrabi, A. (2009). The Role of Religious Valorism in the National Security of the Islamic Republic of Iran. *Hassoun*, *19*(1), 5-22. https://www.noormags.ir/view/en/articlepage/49477/5

[7] Orojloo, H., & Azgomi, M. A. (2017). A method for evaluating the consequence propagation of security attacks in cyber–physical systems. *Future Generation Computer Systems*, *67*, 57-71. https://doi.org/10.1016/j.future.2016.07.016

[8] Colwill, C. (2009). Human factors in information security: The insider threat – Who can you trust these days? *Information Security Technical Report*, *14*(4), 186-196. https://doi.org/10.1016/j.istr.2010.04.004

[9] Fathianpour, F., Hendesi, F., & Ayat, S.S., . (2013, February 14). *Comparison of methods for identifying the behavior of internal employees in the process of attacking computer systems.* 1st payame noor university national conference on information technology & networking, Tabas Branch Payam Noor University, Iran. https://civilica.com/doc/195859/

[10] Jang-Jaccard, J., & Nepal, S. (2014). A survey of emerging threats in cybersecurity. *Journal of Computer and System Sciences*, *80*(5), 973-993. https://doi.org/10.1016/j.jcss.2014.02.005

[11] Tourani, P., Hadavi, M. A., & Jalili, R. (2011, July 4-8). *Access control enforcement on outsourced data ensuring privacy of access control policies.* 2011 International Conference on High Performance Computing & Simulation, Istanbul, Turkey. https://doi.org/10.1109/HPCSim.2011.5999865

[12] Samimi R., P., B. (2017, March 5). *Examining the legal aspects of soft war in cyber space*. National Conference of passive defense in the realm of cyberspace, Maragheh, Iran. https://civilica.com/doc/649521/

[13] Huang, X., Lu, Y., Li, D., & Ma, M. (2018). A Novel Mechanism for Fast Detection of Transformed Data Leakage. *IEEE Access*, *6*, 35926-35936. https://doi.org/10.1109/ACCESS.2018.2851228

[14] Krombholz, K., Hobel, H., Huber, M., & Weippl, E. (2015). Advanced social engineering attacks. *Journal of Information Security and Applications*, *22*, 113-122. https://doi.org/10.1016/j.jisa.2014.09.005

[15] Tounsi, W., & Rais, H. (2018). A survey on technical threat intelligence in the age of sophisticated cyber attacks. *Computers & Security*, *72*, 212-233. https://doi.org/10.1016/j.cose.2017.09.001

[16] Dor, D., & Elovici, Y. (2016). A model of the information security investment decision-making process. *Computers & Security*, *63*, 1-13. https://doi.org/10.1016/j.cose.2016.09.006

[17] Nosratabadi, J., Lashkarian, H., Mardani, M., & Movahhedi, M. (2019). Presenting a Critical Assessment Model for the Armed Forces of the Islamic Republic of Iran. *National Security*, *9*(31), 173-198. https://ns.sndu.ac.ir/article_480.html?lang=en

[18] Prier, J. (2017). Commanding the trend: Social media as information warfare. *Strategic Studies Quarterly*, *11*(4), 50-85. https://www.proquest.com/docview/1972152688

[19] Bowman, C. (2021). *What Are the Predictors of Cyber Power* [Bachelor, James Madison]. Harrisonburg, Virginia. https://commons.lib.jmu.edu/cgi/viewcontent.cgi?article=1135&context=honors202029

[20] Sepehrzadeh, H. (2022). A Method for Assessing the Security Risk in Cyber-Physical Systems with Incomplete Information Using Bayesian Game Theory. *Karafan Quarterly Scientific Journal*, *19*(1), 495-521. https://doi.org/10.48301/kssa.2022.320681.1909

[21] Starr, S. H. (2009). Towards an evolving theory of cyberpower. In C. Czosseck & K. Geers (Eds.), *The Virtual Battlefield: Perspectives on Cyber Warfare*. IOS Press. https://doi.org/10.3233/978-1-60750-060-5-18

[22] Ghoodsi, A. (2014). The Impact of Cyberspace on the National Security of I.R. of Iran and Providing an Approach. *Quarterly Defens Strategy*, *11*(44), 149-186. https://www.magiran.com/paper/1242759

[23] Solani, R., & Das, M.L. (2021). iCOPS: insider attack detection in distributed file systems. *International Journal of Social Computing and Cyber-Physical Systems*, *2*(3), 244-255. https://doi.org/10.1504/ijsccps.2021.117972

[24] Parsons, K., Calic, D., Pattinson, M., Butavicius, M., McCormac, A., & Zwaans, T. (2017). The Human Aspects of Information Security Questionnaire (HAIS-Q): Two further validation studies. *Computers & Security*, *66*, 40-51. https://doi.org/10.1016/j.cose.2017.01.004

[25] Hadlington, L. (2021). The "Human Factor" in Cybersecurity: Exploring the Accidental Insider. In *Research Anthology on Artificial Intelligence Applications in Security*. IGI Global. https://doi.org/10.4018/978-1-7998-7705-9.ch087

[26] Salahdine, F., & Kaabouch, N. (2019). Social Engineering Attacks: A Survey. *Future Internet*, *11*(4), 1-17. https://doi.org/10.3390/fi11040089

[27] Hu, F., Lu, Y., Vasilakos, A. V., Hao, Q., Ma, R., Patil, Y., Zhang, T., Lu, J., Li, X., & Xiong, N. N. (2016). Robust Cyber–Physical Systems: Concept, models, and implementation. *Future Generation Computer Systems*, *56*(1), 449-475. https://doi.org/10.1016/j.future.2015.06.006

[28] Jordan, T. (1999). *Cyberpower: The culture and politics of cyberspace and the Internet*. Routledge. https://www.amazon.com/Cyberpower-culture-politics-cyberspace-Internet/dp/0415170788

[29] Tsigkanos, C., Pasquale, L., Ghezzi, C., & Nuseibeh, B. (2018). On the Interplay Between Cyber and Physical Spaces for Adaptive Security. *IEEE Transactions on Dependable and Secure Computing*, *15*(3), 466-480. https://doi.org/10.1109/TDSC.2016.2599880

[30] Krotofil, M., Cárdenas, A., Larsen, J., & Gollmann, D. (2014). Vulnerabilities of cyber-physical systems to stale data—Determining the optimal time to launch attacks. *International Journal of Critical Infrastructure Protection*, *7*(4), 213-232. https://doi.org/10.1016/j.ijcip.2014.10.003

[31] Krotofil, M., & Cárdenas, A. A. (2013). Resilience of Process Control Systems to Cyber-Physical Attacks. In *Secure IT Systems*. Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-642-41488-6_12

[32] Schellekens, M. (2016). Car hacking: Navigating the regulatory landscape. *Computer Law & Security Review*, *32*(2), 307-315. https://doi.org/10.1016/j.clsr.2015.12.019

[33] Ashibani, Y., & Mahmoud, Q. H. (2017). Cyber physical systems security: Analysis, challenges and solutions. *Computers & Security*, *68*, 81-97. https://doi.org/10.1016/j.cose.2017.04.00 5

[34] Hoehn, A., & Zhang, P. (2016, July 6-8). *Detection of covert attacks and zero dynamics attacks in cyber-physical systems*. 2016 American Control Conference, Boston, Massachusetts, USA. https://doi.org/10.1109/ACC.2016.7524932

[35] Rajamanickam, S., Ramasubramanian, N., & Vollala, S. (2022). Insider Attack Prevention using Multifactor Authentication Protocols - A Survey. In *Applied Information Processing Systems*. Springer Singapore. https://doi.org/10.1007/978-981-16-2008-9_32