قدرت سایبری

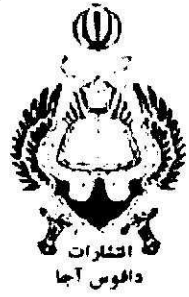
مؤلفه‌های ایجاد قدرت سایبری در یک سازمان نظامی

نویسندگان:

محمد قاسمی

داود آذر

وحید سجادی اصیل



انتشارات دانشگاه فرماندهی و ستاد ارتش جمهوری اسلامی ایران

تابستان ۱۴۰۱

سرشناسه	:	قاسمی، محمد، ۱۳۶۱ -
عنوان و نام پدیدآور	:	قدرت سایبری : مولفه‌های ایجاد قدرت سایبری در یک سازمان نظامی/نویسندگان محمد قاسمی، داود آذر، وحید سجادی‌اصیل ؛ ویراستار سامان آزاد.
مشخصات نشر	:	تهران: ارتش جمهوری اسلامی ایران، دانشگاه فرماندهی و ستاد آجا،انتشارات دافوس، ۱۴۰۱.
مشخصات ظاهری	:	۱۳۱ ص.
شابک	:	۹۷۸-۶۲۲-۷۵۰۴-۹۱-۰
وضعیت فهرست نویسی	:	فیپا
یادداشت	:	کتابنامه: ۱۲۰ - ۱۲۴؛ همچنین به صورت زیرنویس.
عنوان دیگر	:	مولفه‌های ایجاد قدرت سایبری در یک سازمان نظامی.
موضوع	:	شبکه‌های کامپیوتری -- تدابیر ایمنیComputer networks -- Security measures
		فضای مجازی -- تدابیر ایمنیCyberspace -- Security measures
شناسه افزوده	:	آذر، داود، ۱۳۵۵ - سجادی، وحید،۱۳۵۸
شناسه افزوده	:	ایران. ارتش. دانشگاه فرماندهی و ستاد. انتشارات دافوس
شناسه افزوده	:	Staff College. Dafoos Publisher & Iran. Army. Commond
رده بندی کنگره	:	TK۵۱۰۵/۵۹
رده بندی دیویی	:	۰۰۵/۸
شماره کتابشناسی ملی	:	۸۹۷۹۲۶۹
اطلاعات رکورد	:	فیپا

عنوان: قدرت سایبری، مولفه‌های ایجاد قدرت سایبری در یک سازمان نظامی

نویسندگان: محمد قاسمی، داود آذر، وحید سجادی اصیل

طرح روی جلد: میلاد فرهادی

صفحه‌آرایی: حسین بیگدلی شاد

ناشر: انتشارات دافوس

شمارگان: ۱۰۰۰

تعداد صفحات: ۱۳۱ ص

تاریخ نشر: ۱۴۰۱

چاپ اول

لیتوگرافی، چاپ و صحافی: مدیریت چاپ، انتشارات و فصلنامه دانشگاه فرماندهی و ستاد آجا

قیمت: ۴۵۰,۰۰۰ریال

نشانی: تهران، میدان پاستور، خیابان دانشگاه جنگ، دانشگاه فرماندهی و ستادآجا، انتشارات دافوس

تلفن: ۶۶۴۷۰۴۸۶-۰۲۱ ؛ ۶۶۴۱۴۱۹۱ - ۰۲۱

فهرست مطالب

مقدمه:

با توسعه جوامع مجازی در اینترنت، حوزه‌های سرزمینی کاهش‌یافته و الگوهای حکمرانی توسعه پیدا کرده است و الگوی جدیدی برای جوامع و حاکمیت، در حال شکل‌گیری است. نقش دولت‌ها در زندگی مردم کم‌اهمیت‌تر شده است؛ افراد با چندین قرارداد داوطلبانه، زندگی خواهند کرد و با کلیک ماوس در جوامع مختلف وارد می‌شوند. دامنه سایبر ازاین‌جهت منحصربه‌فرد است که ساخته دست بشر اخیر بوده و حتی نسبت به دامنه‌های دیگر نیز با تغییرات سریع فناورانه روبرو می‌شود. جوزف نای اظهار داشت، "جغرافیای فضای مجازی بسیار فراتر از سایر محیط‌ها است. کوه‌ها و اقیانوس‌ها به‌سختی قابل حرکت هستند، اما بخش‌هایی از فضای مجازی را می‌توان با کلیک یک کلید خاموش و روشن کرد".

دولت‌ها همیشه نگران جریان و کنترل اطلاعات بوده‌اند و دوره فعلی اولین دوره‌ای نیست که تحت تأثیر تغییرات چشمگیر فناوری اطلاعات قرار دارد. انقلاب اطلاعاتی کنونی که بعضی آن را "سومین انقلاب صنعتی" نامیده‌اند، مبتنی بر پیشرفت‌های سریع فناوری در رایانه‌ها، ارتباطات و نرم‌افزار است که به نوبه خود منجر به کاهش چشمگیر هزینهٔ ایجاد، پردازش و انتقال اطلاعات شده است. چنین تحولات سایبری، با ایجاد یک انقلاب اطلاعاتی جدید ماهیت قدرت را تغییر داده و انتشار آن را افزایش می‌دهد. کشورها بازیگر غالب در صحنه جهانی خواهند بود، اما صحنه را بسیار شلوغ‌تر و کنترل آن دشوار می‌دانند. بخش بسیار بیشتری از جمعیت هم در داخل و هم در بین کشورها به قدرتی که از طریق اطلاعات حاصل می‌شود دسترسی دارند.

اطلاعات سایبری همچنین می‌توانند در فضای سایبر گردش کنند تا به‌وسیله جذب شهروندان کشورهای دیگر قدرت نرم به‌وجود بیاورند؛ یک برنامه تبلیغات سیاسی در اینترنت مثالی برای این موضوع است. همچنین اطلاعات سایبری می‌توانند به یک منبع قدرت سخت تبدیل شوند، که توانایی وارد کردن صدمه به اهداف فیزیکی در یک کشور دیگر را دارد؛ برای مثال بیشتر صنایع مدرن و خدمات دولتی فرایندهایی دارند که توسط رایانه‌های متصل به سیستم‌های کنترل نظارتی و

جمع‌آوری داده پردازش می‌شود، نرم‌افزار مخربی که به این سیستم‌ها وارد می‌شود، می‌تواند برای خاموش کردن فرایندی که آثار کاملاً فیزیکی دارد برنامه‌ریزی شده باشد؛ برای مثال یک هکر یا یک حکومت، برق یک شهر مانند شیکاگو یا مسکو را قطع کند که این خاموشی گسترده می‌تواند خساراتی بیشتر از بمباران این شهرها وارد کند[1].

به لحاظ نظامی، قدرت سایبر، شاید مهم‌ترین ابزار نوظهور چند دهه گذشته باشد. در حال حاضر اغلب نیروهای مسلح کشورها برای ایمن‌سازی مرزهای سایبر و فراسایبری خود در برابر چنین تحول جدیدی آماده می‌شوند. رهنامه‌های جدید نظامی بر اساس فضای سایبر تدوین می‌شوند. در تمام سطوح منازعه، از شورش‌های داخلی گرفته تا جنگ متعارف، قدرت سایبر، عامل حتمی و گریزناپذیر توانمندی‌های نظامی است و این توانمندی بر پایه فناوری‌های مدرن شکل گرفته است. قدرت سایبر روزبه‌روز خود را به عنوان یک عامل تأثیرگذار در سیاست‌گذاری حوزه‌های ملی از اقدامات ضدتروریستی گرفته تا سامان دادن سیاست، اقتصاد و حتی روابط با سایر کشورها، توسعه می‌دهد[2].

اطلاعات در فضای سایبر به‌راحتی و برای همه به‌صورت یکسان در دسترس هستند. سیستمی که به ارتباطات الکترونیکی متکی است، در صورت تداخل یا ازبین‌رفتن توانایی برقراری ارتباط، می‌تواند بی‌فایده شود. از آنجاکه این اتکا بسیار کلی است، حمله سایبری به زیرساخت‌های اطلاعاتی می‌تواند تأثیرات گسترده‌ای، هم برای ارتش و هم برای جامعه داشته باشد و شناسایی چنین حملاتی که می‌تواند از منابع مختلفی انجام شود، دشوار یا غیرممکن است.

یکی از تهدیدات عصر کنونی، نوع جدیدی از جنگ است که به جنگ ترکیبی معروف است. ماهیت آن به کارگیری تمام ابزارهای غیرمتعارف برای دستیابی به اهدافی است که توسط کاربر

---

[1] Nye, Joseph S. Cyber Power (The future of power in the 21th century). MIT-Harvard Minerva Project, Harvard Kennedy School. 2010 . PP 4-6

[2] زابلی زاده، اردشیر. قدرت بازدارندگی در فضای سایبر دوفصلنامه علمی - پژوهشی رسانه و فرهنگ، سال هشتم شمارهٔ اول، بهار و تابستان ۱۳۹۷، ص ۵۸

ارائه شده است. ابزارهای مورد استفاده در فضای سایبری، قابلیت‌هایی که ارائه می‌دهد تأثیر مکملی بر استراتژی‌های جنگ ترکیبی دارد و یک حلقه بازخورد مثبت ایجاد می‌کند. ارتش برای توصیف فضای سایبری از اصطلاح حوزه پنجم نبرد استفاده می‌کند. فضای سایبر هر چهار حوزه جنگی دیگر را در اطراف خود متحد می کند یا برای همه آنها نقش اساسی دارد. با این حال، اصطلاحات نظامی، هیچ توضیحی در مورد این‌که فضای سایبری واقعاً چیست یا چگونه می‌توان از آن در جنگ ترکیبی استفاده کرد، ارائه نمی‌کنند. فضای سایبر در اصطلاح فنی شبکه‌ای از فناوری و نرم‌افزار دیجیتال است که امکان ایجاد محیطی را فراهم می‌کند که در آن ارتباط بین رایانه‌ها برقرار شود. درهم تنیدگی دنیای واقعی و سایبری در جنگ، عمق جدیدی از نفوذ به حریم خصوصی ملت‌ها، سازمان ها و افراد را ممکن می‌سازد و حتی اسرار ملی را در معرض تهدید قرار می‌دهد. زیرساخت، رفاه اقتصادی یا بیولوژیکی در معرض تهدید دائمی حملات سایبری است که ممکن است هر لحظه رخ دهد. ابزارهای سایبری به طور مداوم در جنگ‌های معاصر استفاده می‌شوند به‌گونه‌ای که می‌توان گفت: خط مقدم در جنگ‌های جدید به روی هر فرد باز شده است، حتی در خانه[1].

مؤلفه‌های متنوعی وجود دارند که تولید کننده قدرت سایبری ملی و سازمانی هستند و توسط سازمان‌های مختلف ارائه می‌شوند؛ اما در کتاب حاضر، هدف نویسندگان بررسی مؤلفه‌های مناسب برای تولید قدرت سایبری در یک سازمان نظامی است لذا سه بعد آفند سایبری، پدافند سایبری و تاب‌آوری سایبری که متناسب با مأموریت سازمان‌های نظامی هستند مورد تأکید و بررسی قرار گرفته است.

فصل اول کتاب به بررسی ادبیات نظری، مفاهیم و اصطلاحات مرتبط با قدرت سایبری پرداخته است. در این فصل مفاهیم قدرت، فضای سایبر، ارتباط این فضا با سایر فضاها و لایه‌های مختلف آن پرداخته شده است در ادامه قدرت سایبری، قدرت سایبری نظامی تشریح شده است.

---

[1] Tsiklauri, Giorgi. Hybrid Warfare in Cyber domain: Case Study of hybrid threats in cyberspace. CHARLES UNIVERSITY, FACULTY OF SOCIAL SCIENCES, Institute of Political Studies, 2021, PP 7-10