Quarterly Journal of Hamedan Police Science

Journal homepage: http://hamedan.jrl.police.ir/

57 Vol.8, No.29, Summer 2021

Command Network Model and Soft Power Control among Armed Forces

Mahdi Naghavi
*MA in Information and Security, Amin University, Tehran, Iran.
mehdin418@gmail.com
(Corresponding Author).

Received: 2021/04/28
Accepted: 2021/09/07

DOI:
10.22034/hpsj.2021.207648.1043

ABSTRACT

Today, due to the expansion of computer systems and networks in all areas of infrastructure, communication, and information with the existence of some properties such as unlimited geographical boundaries and pervasive use, easy and fast services using up-to-date technology and information have come true. On the other hand, in line with this fast progress, the crime has been appearing from the real environment to cyberspace. The spread of crime, cyber-attacks, and destructive activities are observed in this space every day. Observing the traces of these cases using all tools causes the collection of detection equipment, operational and passive countermeasures, cyber operations, electronic warfare, and etc. in the ground, sea, and air base way to be integrated in a basic structure for specific purposes. These purposes are diverse and in addition to speed and acceleration and freedom of action in space, land, and sea, they also have their own tricks and deceptions in cyberspace, social networks, and psychological operations. Commanding and controlling soft power in the armed forces in the form of a unique and extensive network are able to achieve these purposes only through unity, effort, coordination, common language, the establishment of interactions, and exchanges of information and operations with other states and military organizations. Comprehensive, united and unified network in a coherent structure is one of the characteristics of this network. Its distinctive feature is the collection of information and news, its processing and coordination, adaptation and integration of information, as well as the dissemination of the news and information to all command centers and soft power control required in terms of authorized access to the information. In this research, a new model of soft power commanding and controling for the armed forces is provided.

Keywords: Soft Power, Control Command, Integration and Adaption of Information, psychological operations.

►**Citation (Vancouver):** Naghavi M. Command Network Model and Soft Power Control among Armed Forces. Quarterly J Hamedan Police Sci. Summer 2021; 8(2):57-65.

►**Citation (APA):** Naghavi, M. (Summer 2021). Command Network Model and Soft Power Control among Armed Forces. *Quarterly Journal of Hamedan Police Science*, *8*(2), 57-65.

الگوی شبکهٔ فرماندهی و کنترل قدرت نرم در نیروهای مسلح

مهدی نقوی
– کارشناس ارشد اطلاعات، دانشگاه علوم انتظامی، تهران، ایران.
mehdin418@gmail.com
(نویسنده مسؤول).

چکیده

امروز، با گسترش سیستم‌ها و شبکه‌های رایانه‌ای در تمامی عرصه‌های زیرساختی، ارتباطی و اطلاعاتی با وجود ویژگی‌هایی نظیر مرزهای جغرافیایی نامحدود و کاربرد فراگیر، انتقال خدمات سریع و آسان با بهرگیری از فناوری و اطلاعات روز میسر شده است. ازطرفی، هم‌سو با این پیشرفت برق‌آسا، بستر جرایم از محیط حقیقی پا به فضای سایبری باز نموده و هر روز شاهد گسترش جرایم، حملات سایبری و فعالیت‌های مخرب در این فضا هستیم. رهگیری این موارد با تمامی ابزار موجب می‌گردد تا مجموعهٔ تجهیزات کشف، جمع‌آوری شوند و مقابله اعم از عامل و غیر عامل، عملیات سایبری، جنگ الکترونیک و ... به‌صورت زمین‌پایه، دریاپایه و هواپایه در یک ساختار اساسی برای اهداف مشخص تجمیع گردند. این اهداف متنوع است و علاوه‌بر سرعت و شتاب و داشتن آزادی عمل در فضا، زمین و دریا ترفندها و فریب‌کاری خاص خود را در فضای مجازی، شبکه‌های اجتماعی و عملیات روانی نیز دارا هستند. فرماندهی و کنترل قدرت نرم در نیروهای مسلح درقالب یک شبکهٔ واحد و گسترده تنها با وحدت، تلاش، هماهنگی، هم‌زبانی و برقراری تعاملات و تبادلات اطلاعاتی و عملیاتی با سایر سازمان‌های کشوری و لشکری قادر است به اهداف یاد شده دست یابد. جامع، متحد و واحدبودن شبکه در ساختاری منسجم ازجمله خصوصیات این شبکه است. مشخصهٔ بارز آن تجمیع اطلاعات و اخبار، پردازش و هماهنگی آن، تطبیق و تلفیق اطلاعات و همچنین انتشار این اخبار و اطلاعات به تمامی مراکز فرماندهی و کنترل قدرت نرم مورد نیاز برحسب میزان دسترسی مجاز عناصر به اطلاعات مذکور است. در این پژوهش، الگوی نوین فرماندهی و کنترل قدرت نرم برای نیروهای مسلح ارائه شده است.

کلیدواژه‌ها: قدرت نرم، فرماندهی کنترل، تلفیق و تطبیق اطلاعات، عملیات روانی.

نوع مقاله: پژوهشی
صص: ۵۷-۶۵.
تاریخ دریافت: ۱۴۰۰/۰۲/۰۸
تاریخ پذیرش: ۱۴۰۰/۰۶/۱۶
شناسه دیجیتال (DOI):
10.22034/hpsj.2021.207648.1043

◄**استناد (ونکوور):** نقوی م. الگوی شبکهٔ فرماندهی و کنترل قدرت نرم در نیروهای مسلح. فصلنامهٔ علمی دانش انتظامی همدان. تابستان ۱۴۰۰؛ ۸(۲): ۵۷-۶۵.

◄**استناد (APA):** نقوی، م. (تابستان ۱۴۰۰). ساخت و اعتباریابی آزمون فرافکن تصویری به منظور سنجش اختلال PTSD در جانبازان جنگ و ناجا. *فصلنامهٔ علمی دانش انتظامی همدان*، ۸(۲)، ۵۷-۶۵.

مقدمه

یکی از مهم‌ترین عرصه‌های نوظهور در امور نظامی و انتظامی که با ورود بشر به عصر اطلاعات، متولد گردیده است، جنگ سایبری و اطلاعاتی است. این نوع جنگ اساسا رویکردها، ابزارها، راه‌کارها، ترفندها و نتایج خاص خود را دارد. جنگ اطلاعاتی یک اصطلاح نسبتا جدید است که طی سال‌های گذشته به واژه‌نامهٔ اصطلاحات نظامی وارد شده است. البته، استفاده از واژهٔ اطلاعات در جنگ قدمتی طولانی دارد. ظهور اصطلاح جنگ اطلاعاتی و اهمیت روزافزون آن با انقلاب اطلاعات ارتباط مستقیم دارد. از این‌رو، فضای سایبری عبارتی است که در دنیای اینترنت، رسانه و ارتباطات بسیار شنیده می‌شود. واژهٔ «سایبر» از لغت یونانی «Kybernetes» به‌معنای «راهنما» مشتق شده است.

نخستین بار اصطلاح "سایبرنتیک" توسط ریاضیدانی به نام «نوربرت وینر[1]» در کتابی با عنوان «سایبرنتیک و کنترل در ارتباط بین حیوان و ماشین» در سال ۱۹۴۸ به‌کار برده شد. سایبرنتیک علم مطالعه و کنترل سازوکارها در نظام‌های انسانی، ماشینی و رایانه‌ایی است. سایبر، پیشوندی است برای توصیف یک شخص، یک شیء، یک عقیده و یا یک فضا که مربوط به دنیای کامپیوتر و اطلاعات است. درطی توسعهٔ اینترنت واژه‌های ترکیبی بسیاری از واژهٔ «سایبر» به‌وجود آمده است که به تعدادی از آن‌ها اشاره می‌کنیم: فضای سایبر، شهروند سایبر[2]، پول سایبر[3]، فرهنگ سایبر[4]، راهنمایی فضای سایبر[5]، تجارت سایبر[6]، کانال سایبر[7] و ... عبارت «فضای سایبر» را نخستین بار ویلیام گیبسون[8] نویسندهٔ داستان علمی-تخیلی کتاب «نورومنسر[9]» در سال ۱۹۸۴ به‌کار برد. فضای سایبر در معنا به مجموعه‌هایی از ارتباطات درونی انسان‌ها ازطریق رایانه و مسائل مخابراتی بدون درنظرگرفتن جغرافیای فیزیکی اطلاق می‌شود. یک نظام برخط، نمونه‌ای از فضای سایبر است که کاربران آن می‌توانند ازطریق ایمیل با یک‌دیگر ارتباط برقرارکنند.

برخلاف فضای واقعی، در فضای سایبری نیاز به جابه‌جایی‌های فیزیکی نیست و کلیهٔ اعمال فقط ازطریق فشردن کلیدها یاحرکات ماوس صورت می‌گیرد.

جنگ سایبری و اطلاعات، اصول جنگی جدیدی را جایگزین اصول قدیمی نموده‌اند. نوع نیروهایی که در این گونه جنگ‌ها شرکت می‌کنند، نحوهٔ استفاده از آن‌ها و حتی یورش به‌سوی دشمن و استراتژی جنگی با گذشته تفاوت‌های بسیار عمیقی پیدا کرده است. امروز، تصمیم‌گیری درمورد تعداد، نوع و مکان استفاده از حسگرها، کامپیوترها، شبکه‌ها و بانک‌های اطلاعاتی که در جنگ مورد استفاده قرار می‌گیرند همان اهمیتی را پیدا کرده که در جنگ جهانی دوم درمورد زمان و نحوهٔ استفاده از بمب‌افکن‌ها در پشت خط مقدم دشمن مطرح می‌شد.

اخلال‌گران رایانه‌ای دارای اهداف گوناگونی هستند. برخی با هدف کسب پول و سود، به شبکه‌ها نفوذ می‌کنند و با هک‌کردن کارت‌های اعتباری، پول سرشاری به جیب می‌زنند. بعضی دیگر هدفشان سرگرمی، تفریح و به رخ کشیدن توان فنی و رایانه‌ای‌شان است. اما، بسیاری از هکرها هم دارای گرایشات سیاسی یا اجتماعی می‌باشند. به این گروه از هکرها «Actives» گفته می‌شود. هدف عمدهٔ این گروه از نفوذکننده‌ها، اخلال در سیستم‌های رایانه‌ای سازمان‌ها، وزارتخانه‌ها یا شبکه‌های مرتبط با دولت خاصی است. شبکهٔ رایانه‌ای ارتش، وزرات دفاع، وزرات خارجه، پلیس، کاخ ریاست جمهوری، شبکهٔ رادیو و تلویزیون، بانک مرکزی، احزاب سیاسی، مجلس، کنگره و سایر دستگاه‌های سیاسی از عمده‌ترین اهداف این گروه به‌شمار می‌روند.

این نوع جنگ‌ها در جهان امروز بسیار متداول است. برای نمونه، دولت آمریکا ماه‌ها پیش از شروع جنگ علیه عراق درراستای جنگ اطلاعاتی و عملیات روانی خود علیه

1. Norbert Wiener
2. Cybercitizen
3. Cyber Cash
4. Cyber Culture
5. Cyber Coach
6. Cyber Business
7. Cyber Channel
8. William Gibson
9. Necromancer

این کشور، استراتژی معینی را تحت عنوان «استراتژی رخنه و ایجاد اختلال در سیستم‌های رایانه‌ای دشمن» تصویب کرده بود. براساس این استراتژی، ماه‌ها و هفته‌ها پیش از شروع جنگ، باید سیستم‌های ارتباطی و رایانه‌ای عراق شناسایی می‌شد و عملیات لازم برای نفوذ و ایجاد اختلال در عمل‌کرد آن‌ها صورت می‌گرفت. روزنامهٔ واشنگتن‌پست در گزارشی که دو هفته پیش از شروع جنگ در عراق منتشر کرد، فاش نمود: آمریکا سرگرم بررسی و طرح‌ریزی برای حملات اینترنتی علیه کشورهایی مانند عراق است. این حملات قرار بود پیش از شروع عملیات نظامی یا هم‌زمان با آن صورت گیرد. سایت اینترنتی BBC دو روز پس از انتشار گزارش چنین نوشت: "در هر گونه نبرد اینترنتی علیه عراق باید نقشی را که رایانه‌ها در ادارهٔ امور این کشور ایفا می‌کنند مد نظر قرار داد".

وینستون چرچیل در جنگ جهانی دوم از پیدایش جنگ الکترونیک به‌عنوان «نبرد جادویی» نام برد و اینک پس از ۵۵ سال از گفتار «نبرد جادویی» در عرصهٔ اینترنت تحقق یافته است. به موازات آن‌که دولت‌ها و شرکت‌ها سعی می‌کنند تا هرچه بیشتر شبکه‌های رایانه‌ای را تحت نفوذ و کنترل خود درآورند، شبکه اینترنت به محیطی مناسب برای تروریست‌های رایانه‌ای، فعالان سیاسی و نفوذگران اینترنتی و حتی خود دولت‌ها تبدیل شده است. در سال ۱۹۹۸ وزارت دادگستری و پلیس فدرال آمریکا به‌طور مشترک واحد جدیدی به نام «مرکز پشتیبانی زیرساخت ملی» تشکیل داد که وظیفهٔ آن تقویت توان دفاعی ایالات متحده در مقابل تروریسم رایانه‌ای و سایر تهدیدات الکترونیک است.

یک نمونه جنگ شبکه‌ای را می‌توان در مبارزهٔ ارتش آزادی‌بخش ملی زاپاتیستا و دولت مکزیک یافت. در اولین روز سال ۱۹۹٤، ارتش آزادی‌بخش ملی زاپاتیستا، شش شهر را در چیاپاس اشغال کردند و علیه دولت مکزیک اعلان جنگ نمودند، خواهان تغییراتی شدند و سرانجام به یک پیکار رسانه‌ای جهانی دست زدند. آن‌ها خواهان اصلاحات سیاسی، اقتصادی و اجتماعی ازجمله حقوقی برای بومیان، انتخابات مشروع و منصفانه و لغو مقرارت حاکم بر اجارهٔ زمین شدند. ارتش مکزیک سرزمین‌های اشغالی را پس گرفت، اما زاپاتیست‌ها سعی کردند از دارابودن زاپاتیست‌ها و حامیان آن‌ها از اینترنت برای سخن‌گفتن دربارهٔ وضعیت خود و هماهنگ‌کردن فعالیت‌ها استفاده کنند. یک گروه از حامیان نیویورکی به نام «تاتر مزاحمت الکترونیکی»، حمله به سایت زدیلو رئیس جمهور مکزیک را سازمان دادند. در ۱۰ آوریل ۱۹۹۸ شرکت‌کنندگان در حملهٔ موتورهای جستجوی شبکهٔ وب خود را به سایتی با نرم‌افزار فلادنت که سایت هدف را با ترافیک بمباران می‌کرد، وصل کردند. گروه تاتر مزاحمت الکترونیکی برنامه‌ریزی کرد که در ۱۰ مه، حمله را تکرار کند، اما وقتی گروه حقوق بشر مستقر در مکزیک اعتراض نمود، برنامهٔ خود را تغییر داد. در نه سپتامبر این گروه دوباره به سایت رئیس جمهور زدیلو و سایت‌های پنتاگون و بورس فرانکفورت حمله کرد.

مطالعات بسیاری نیز در این حوزه صورت گرفته است. سابقهٔ نظریهٔ جنگ اطلاعات در آمریکا به سال ۱۹۷۰ برمی‌گردد، یعنی هنگامی که دکتر "تامرونا" اولین بار این واژه را به‌کار برد. کارهای انجام‌شده در این زمینه تا سال ۱۹۹۰ که وزارت دفاع آمریکا نظریهٔ جنگ فرماندهی و کنترل را به‌عنوان بخشی از جنگ اطلاعات در حوزهٔ وسیع‌تری مطرح نمود، انتشار پیدا نکرد. بعد از انتشار کتاب «جنگ و ضد جنگ» نویسنده‌های متعددی مقالاتی درخصوص راهبرد جنگ خلیج فارس بر مبنای اطلاعات منتشر نمودند.

کلنل آلن کمپن در کتاب «اولین جنگ اطلاعات» بحث به‌کارگیری سامانهٔ C4I در جنگ خلیج فارس و مزایای اختلاف اطلاعاتی به‌وجودآمده و ایجاد نتایج فریب، مانور و سرعت را مطرح نمود. نیل مانرو در کتاب «سرعت و مرگ» درگیری الکترونیکی و جنگ نوین اصول جنگ الکترونیک و اثرات آن در فرماندهی و کنترل را به‌صورت مبسوط ارائه نمود. در همین ایام، ویت شوارتا در کتاب «جنگ نوین اطلاعات: هرج و مرج در ابرآزادراه اطلاعات»، تهدیدهای وسیع در شبکهٔ جهانی اطلاعات را بررسی کرده است.

کنفرانس‌های متعددی که از سال ۱۹۹۳ در زمینهٔ جنگ اطلاعات و سایبری توسط صنایع دفاعی و حفاظت اطلاعات ارائه شده به ایجاد یک فضای باز نقد و بررسی جنگ اطلاعات و سایبری کمک نموده است. در همین زمان هیأت علوم دفاعی وزارت دفاع ۲ پروژهٔ اصلی در این زمینه را به اجرا گذاشت و لزوم سرمایه‌گذاری گسترده در زمینه-های ساماندهی در IW، ایجاد امنیت برای DII و تحقیق توسعه در بخش IW را توصیه نمود.

درحال حاضر، کلیهٔ ساختار فرماندهی و کنترل قدرت نرم نیروهای مسلح با بهره‌گیری از توان تخصصی کارکنان و با جمع‌آوری و یک‌پارچه‌سازی سنتی و بعضا استفاده از سیستم‌های جزیره‌ای انجام می‌گیرد. فرماندهی و کنترل قدرت نرم با استفاده از ظرفیت و پتانسیل کلیهٔ سازمان‌های تخصصی در نیروهای مسلح و همچنین برقراری تعاملات و تبادلات لازم با سایر سازمان‌های لشکری و کشوری می‌تواند اقدام به جمع‌آوری، تحلیل و ارائهٔ اطلاعات و گزارشات مورد نیاز نموده و فرمانده را جهت اتخاذ تصمیم مناسب در مواجهه با مسائل سایبری، فضای مجازی و عملیات روانی یاری نماید. فقدان مراکز فرماندهی و کنترل هوشمند در این مهم منجربه بروز برخی کاستی‌ها شده که در ادامه به تعدادی از این کاستی‌ها اشاره می‌شود. **این کاستی‌ها عبارتند از:** روش و تجهیزات موجود دربرابر مأموریت جدید نیرو های مسلح در حوزهٔ قدرت نرم، ازقبیل تنوع تهدیدات فضای سایبری، تنوع اقدامات مرتبط با عملیات روانی، تنوع علوم شناختی، تنوع رسانه‌ها به‌علت عدم کفایت سیاست‌گذاری **جریان اطلاعات** و افزایش سطح نظارتی در حوزهٔ فضای مجازی، شبکه‌های اجتماعی، عملیات روانی و علوم شناختی و همچنین فقدان سامانهٔ فرماندهی و کنترل هوشمند مرتبط با قدرت نرم با آسیب‌های جدی.

با توجه به تدابیر ابلاغی مبنی‌بر اهمیت بالای ساعات اول تهدیدات نرم احتمالی و نیاز به تدبیر در خصوص کاهش خسارات ساعات اولیهٔ تهدید نرم، موضوع تشخیص تهدیدات اولیه و شروع جنگ از اهمیت ویژه‌ای برخوردار است. بنابراین، توجه به ویژگی هوشیاربودن شبکهٔ فرماندهی و کنترل با اجتناب از استهلاک شبکه و تجهیزات در طراحی و معماری شبکهٔ فرماندهی و کنترل حائز اهمیت ویژه است. ضرورت دارد ساختار و الگوی نوین فرماندهی و کنترل به‌گونه‌ای که بتوان سناریوهای دفاعی مختلف را در شرایط دفاعی متفاوت اجرا نمود، تدوین شوند و امکان بهره‌مندی از مزایای ساختار درراستای نیل به نیازها و ضرورت‌های ذیل ارائه شود:

- معماری، طراحی، تولید، تجهیز و تکمیل کلیهٔ یگان‌های نیروهای مسلحبه سامانه‌ها و زیر سامانه‌های فرماندهی و کنترل قدرت نرم.
- دست‌یابی به شبکهٔ ارتباطی امن و پایدار مابین مراکز فرماندهی و کنترل قدرت نرم (ثابت و سیار)، سامانه‌ها و زیرسامانه‌ها، حساسه‌ها و تجهیزات مرتبط با جنگ نرم.
- بهره‌گیری از کلیهٔ اطلاعات، اخبار، رویدادها، موضوعات عملیات روانی در شبکه‌های اجتماعی، فضای مجازی و همچنین کلیهٔ اطلاعات مؤثر در نیروهای مسلح به‌صورت بلادرنگ مانند اطلاعات سامانه‌ها، مراکز مدیریت عملیات روانی نیروها، اطلاعات شبکه‌های اجتماعی مرتبط با سایر سازمان‌ها (فتای ناجا، سایبری سپاه و ...).
- امکان ارائهٔ تدابیر و دستورات و در نهایت هدایت مراکز فرماندهی و کنترل قدرت نرم نیرویی/منطقه‌ای ازطریق بررسی گزارشات تحلیلی به‌صورت برخط در مناطق تحت شبکهٔ فرماندهی و کنترل با تأکید بر استقلال عملکرد نیروها.
- امکان هدایت و کنترل تجهیزات جنگال و پدافند غیر عامل کشوری و لشکری.

در این پژوهش، به‌دنبال پاسخ به این پرسش اصلی هستیم که «الگوی مناسب نیازمندی‌های فرماندهی و کنترل قدرت نرم نیروهای مسلح چگونه است؟»

اهداف پژوهش

هدف اصلی این پژوهش عبارت است از: «معماری، طراحی، پیاده‌سازی و توسعهٔ شبکهٔ یک‌پارچهٔ فرماندهی و کنترل قدرت نرم نیروهای مسلح»

اهداف فرعی پژوهش نیز در زیر آمده‌اند:

- جمع‌آوری و به‌کارگیری کلیهٔ اطلاعات مؤثر در افزایش قدرت نرم نیروهای مسلح و کمک‌گیری از کلیهٔ منابع اطلاعاتی داخل و خارج از نیروهای مسلح،
- توزیع و انتشار مؤثر اطلاعات در شبکه،
- دسترسی بر اساس نیاز کلیهٔ اقدام‌گرها به اطلاعات و تدابیر تزریق‌شده در شبکه،
- تحت پوشش قراردادن تعداد و تنوع زیاد تجهیزات، شبکه ها و رسانه‌ها،
- دریافت و تأثیردهی بلادرنگ تحلیل اطلاعاتی ازطریق داشبوردهای نرم‌افزاری و تدبیر عملیاتی کاربران باتجربه در شبکه و ارائهٔ گزارشات تحلیلی در حوزه‌های فضای مجازی، اجتماعی و عملیات روانی،
- ایجاد شرایط امکان کنترل و هدایت کلیهٔ مراکز فرماندهی و کنترل قدرت نرم نیروهای مسلح اعم از مراکز فرماندهی و کنترل قدرت نرم نیرویی.

روش پژوهش

هنگام بررسی الگوی جنگ‌های آینده باید فضای مفهومی چنین جنگ‌هایی را به‌خوبی تشریح کرد. البته، ضرورت دارد، پیش از ترسیم این نقشهٔ مفهومی، افق آینده‌پژوهی صریحا تعیین شود. زیرا، با توجه به تحولات شتابانی که در حوزه‌های مختلف تمدن نوین رخ می‌دهند، هر گونه پیش‌بینی یا برآورد دربارهٔ وضعیت جهان در دهه‌های آینده احتمالا با خطای بالا همراه خواهد بود. به‌عنوان مثال، علی‌رغم گسترش و نفوذ حیرت‌انگیز فناوری اطلاعات و ارتباطات و ملموس‌بودن پیامدها و تأثیرات این فناوری بر چیستی و چگونگی اصول جنگ، امروز هیچ کارشناسی قادر نیست که پیامدها و تأثیرات پیشرفت‌های انقلابی در زمینهٔ فناوری نانو و فناوری زیستی را که عصر طلائی آن‌ها شاید از سال ۲۰۲۰ به بعد آغاز شود، بر جنگ‌های دهه‌های آینده به‌درستی پیش‌بینی کند. درنتیجه، افق آینده‌پژوهی دراین گزارش حداکثر تا سال ۲۰۱۵ ادامه یافته و ترجیحا درباره افق‌های دورتر سکوت می‌کند. مفاهیم عملیاتی نوین که در آیندهٔ نزدیک شاهد ظهور آن‌ها خواهیم بود، به روابط و نحوهٔ تعامل عناصر کلیدی جنگ‌های آینده بستگی خواهند داشت.

در نظریهٔ جنگ نسل چهارم که مبتنی‌بر نظریه‌ها یا فناوری‌های نو است، تسلحیات هدایت مستقیم انرژی، روباتیک و عملیات‌های رسانه‌ای، و نهایتا تروریسم معرفی شده‌اند که این‌ها به مفاهیم جنگ کلاسیک پیشرفته، جنگ روباتی، جنگ روانی و جنگ ناهم‌تراز[1] منجر می‌شوند.

همچنین، در نظریهٔ جنگ موج سوم که بیشتر در جامعهٔ اطلاعات‌محور مطرح شده و جنگ‌افزارهای هدایت‌پذیر دقیق، روبات‌ها و فناوری غیر کشنده، تسلیحات هدایت مستقیم انرژی و ویروس‌های رایانه‌ای کانون تمرکز آن است، مفاهیم جنگ سایبری[2]، جنگ کلاسیک پیشرفته و جنگ روباتی مورد تأکید قرار می‌گیرند.

نهایتاً، از نظریهٔ جنگ عصر چهارم که به دو صورت سبک غربی مبتنی‌بر فناوری‌های پیشرفته، تسلیحات هدایت‌پذیر دقیق، جنگ اطلاعاتی، جنگ‌افزارهای غیر کشنده، یگان‌های جنگی روباتیک، تسلیحات هدایت‌کنندهٔ انرژی و سبک غیر غربی مبتنی‌بر تروریسم معرفی می‌شود، می‌توان مفاهیم جنگ کلاسیک پیشرفته، جنگ سایبری، جنگ روباتی و جنگ ناهم‌تراز را استخراج کرد.

1. Asymmetric Warfare
2. Cyber Warfare

درواقع، هر سه نظریهٔ مذکور به‌طور مستقیم یا غیر مستقیم بر اهمیت پنج مفهوم جنگی زیر تأکید می‌کنند:

≠ جنگ کلاسیک پیشرفته (اعم از متعارف و غیر متعارف)

≠ جنگ روباتی

≠ جنگ روانی

≠ جنگ سایبری

≠ جنگ ناهم‌تراز

شایان ذکر است، جنگ ناهم‌تراز به خودی خود یک نوع جنگ متمایز محسوب نمی‌شود، بلکه باید آن را یک رویکرد یا نگاه متفاوت به عملیات جنگی تلقی کرد. درواقع، در یک جنگ ناهم‌تراز، تفاوت قابل توجهی بین قوای دو طرف وجود دارد، به همین دلیل، می‌توان با توجه به توانمندی‌ها و نقاط ضعف مهاجم و مدافع از هر چهار نوع جنگ کلاسیک پیشرفته، روباتی، روانی و سایبری بهره جست. به‌بیان دیگر، جنگ‌های ناهم‌تراز اساسا دربرگیرندهٔ روش‌هایی‌اند که در سطوح مختلف از مفاهیم و اصول جنگ کلاسیک پیشرفته (یا بدون کاربرد سلاح‌های کشتار جمعی)، جنگ روانی، جنگ سایبری و جنگ روباتی تبعیت می‌کنند.

علاوه‌بر این، باید خاطرنشان کرد که در تعاریف رایج ارائه‌شده برای جنگ ناهم‌تراز بیشتر عدم توازن قدرت بین طرفین درگیر پررنگ شده و اساسا انجام عملیات ناهم‌تراز به طرف ضعیف‌تر نسبت داده می‌شود. درحالی‌که اگر تعریف جنگ ناهم‌تراز را با توجه به ویژگی مهم «تاثیر نامتناسب[1]» (یعنی، تحقق اهداف استراتژیک ازطریق اقدامات غیر استراتژیک) گسترش دهیم، درمی‌یابیم که انتخاب این رویکرد متفاوت به جنگ لزوما در پرتو موازنهٔ قدرت نظامی انجام نمی‌شود. بنابراین، اگر یک طرف قوی تشخیص دهد که می‌تواند با استفاده از روش‌های ناهم‌تراز به هدف استراتژیک خود، یعنی تسلیم‌شدن دشمن و ازبین‌بردن اراده و روحیهٔ جنگی او دست یابد، قطعا به رویکردهای ناهم‌تراز متوسل خواهد شد.

در جنگ‌های آینده نیز مانند جنگ‌های گذشته اصولاً تحقق دو هدف بنیادی در دستور کار قرار می‌گیرند که عبارتند از:

≠ تسلیم‌شدن دشمن

≠ نابودشدن دشمن

نمودار زیر جنبه‌های مختلف تهدیدات سایبری را نشان می‌دهد:

شکل ۱- جنبه‌های مختلف تهدیدات سایبری

1. Disproportionate Effect

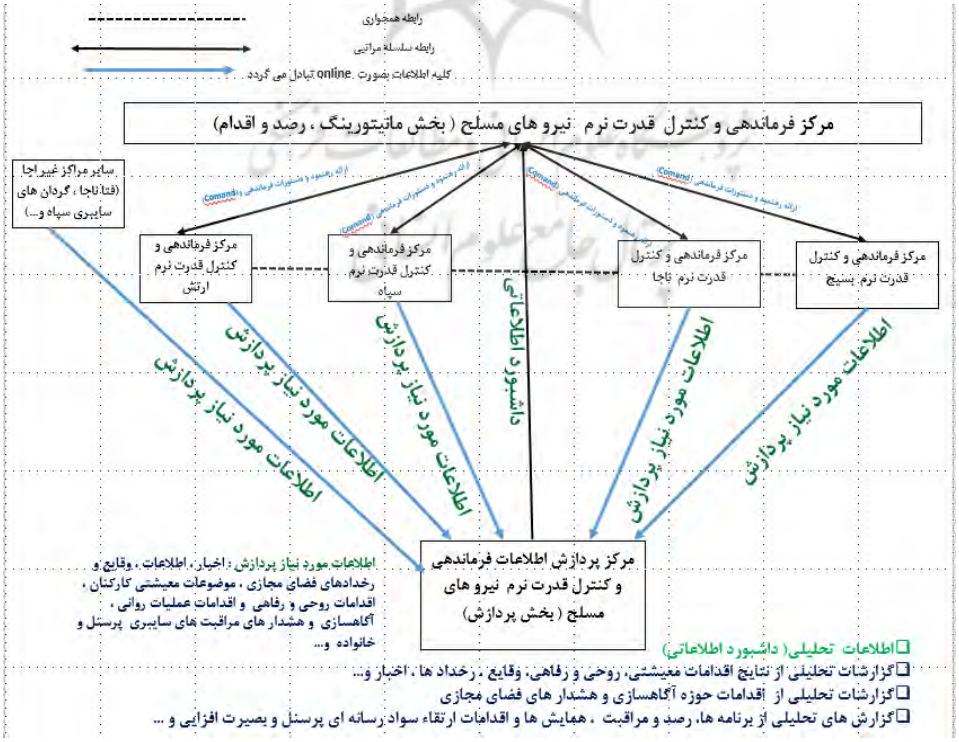
هر گونه ضعف یا قوت در زیرساخت‌ها و نرم‌افزارهای حیاتی فناوری اطلاعات و ارتباطات به ضعف یا قوت در مفاهیم مختلف جنگی می‌انجامد. درنتیجه، نظام فناوری اطلاعات و ارتباطات بر همهٔ انواع جنگ تأثیرگذار است. اما، عکس این رابطه لزوما همیشه صادق نیست. برای نمونه، جنگ روانی هیچ تأثیر معینی بر نظام فناوری اطلاعات و ارتباطات ندارد.

یافته‌ها

اکثریت مصاحبه‌شوندگان، جنگ اطلاعاتی، رایانه‌ای و شبکه‌محور را یکی از ابعاد جنگ‌های نوین و آینده دانسته و نیاز به مجهزشدن به ابزار آفندی و پدافندی مناسب را یک ضرورت اجتناب‌ناپذیر می‌دانند. در این راستا، ایجاد ساختار یگانی مناسب، همراه با نیروهای کیفی (دارای توان فنی و علمی بالا در علوم سایبری) جهت اجرای عملیات در این فضا، دست‌یابی به ابزارهای ویژهٔ این نوع جنگ و همچنین ایجاد بسترهای خاص را از ملزومات شمرده و اعتقاد دارند که با ایجاد مرکز فرماندهی و کنترل قدرت نرم مرکب از کارشناسان مجرب و خبره در زمینهٔ فناوری اطلاعات (محوریت اجرا) و عملیاتی (مشاوره) جهت شناسایی و ارزیابی نقاط آسیب‌پذیر شبکهٔ فرماندهی و کنترل و مشخص‌نمودن درگاه‌های ورودی و خروجی اطلاعات نظارت و بررسی مداوم اطلاعات جابه‌جا شده (پایش)، ایجاد ساختار و به‌کارگیری نرم‌افزارهای تخصصی در این زمیه و استفاده از سامانهٔ مدیریت امنیت آموزش و بهره‌گیری از کارکنان مجاز و رعایت مسائل و نکات امنیتی دفاع سایبری قابل اجرا است.

شاخص‌های اصلی در تبین نیازهای فرماندهی و کنترل قدرت نرم شامل مراکز نیرویی، سطوح فرماندهی و کنترل، سامانه‌ها و نرم‌افزارهای تخصصی در این زمینه است که در این پژوهش نهایتاً به ساختار زیر می‌رسیم:

شاخص‌های اصلی در تبین نیازهای فرماندهی و کنترل قدرت نرم شامل مراکز نیرویی، سطوح فرماندهی و کنترل، سامانه‌ها و نرم‌افزارهای تخصصی در این زمینه است که در این پژوهش نهایتاً به ساختار زیر می‌رسیم:



شکل ۲- شاخص‌های اصلی در تبیین نیازهای فرماندهی و کنترل قدرت نرم نیروهای مسلح

بحث و نتیجه‌گیری

چنان‌که قبلا نیز اشاره شد، کشورهایی که مراحل ابتدایی بهره‌برداری از فناوری اطلاعات را پشت سر می‌گذارند، به‌تدریج از موقعیت عدم آسیب‌پذیری نسبی به موقعیت، شامل درجه‌ای از آسیب‌پذیری حرکت می‌کنند.

چنین احتمال می‌رود که در آیندهٔ نزدیک بررسی‌های بین‌المللی دربارهٔ الگوها، مزایا، محدودیت‌ها و شرایط جنگ اطلاعاتی و سایبری نهایتا اکثر کشورهای جهان را به‌سمت طرح‌ریزی پدافندی اطلاعاتی سوق داده و آن‌ها را ملزم به ارتقای توان دفاع اطلاعاتی و شبکه‌ای رایانه‌ای دربرابر آفندهای آن به‌ویژه ازسوی ایالات متحدهٔ آمریکا کند. ازاین‌رو، بعید نیست که یک بازار بین‌المللی برای طراحی و توسعهٔ ابزارهای قوی پدافند سایبری ظهور کند که درطی زمان و حتی درطی یک شبانه‌روز اکثر ابزارها و تکنیک‌های آفندی را خنثی کنند.

پدافند شبکه‌ای فرماندهی و کنترل قدرت نرم شامل اقداماتی می‌شود که به‌منظور حفاظت، پایش[1]، تحلیل، آشکارسازی و واکنش به فعالیت‌های غیر مجاز در سیستم‌ها و شبکه‌های فضای مجازی، شبکه‌های اجتماعی و مجموعه عملیات روانی انجام می‌شود. قدرت نرم آفندی و پدافندی شامل اقداماتی می‌شود که به‌منظور پرهیز، آشکارسازی و منحرف‌سازی اقدامات مستقیم یا غیر مستقیم دشمن علیه سیستم‌های اطلاعاتی خودی انجام می‌گیرند. در پدافند شبکهٔ فرماندهی و کنترل بر آشکارسازی و تطبیق، یکسان‌سازی و شناسایی اهداف و انجام تدبیرهای لازم اشاره دارد.

منابع

۱. اسکیلز، رابرت. (۱۳۸٤). *جنگ آینده، ترجمه عبدالمجید حیدری*. تهران، انتشارات سپاه پاسداران انقلاب اسلامی.

۲. موسسه آموزشی و تحقیقاتی صنایع دفاعی. (۱۳۸٤). *طرح فراسازمانی فرماندهی و کنترل، چشم‌انداز مشترک ارتش آمریکا در افق ۲۰۲۰*. تهران، موسسه آموزشی و تحقیقاتی صنایع دفاعی.

۳. عقلمند، احمد. (۱۳۸۲). *مروری بر تاریخ تحولات فناوری سلاح‌های نظامی*. تهران، امیرکبیر.

٤. مکنزی، کنت. (۱۳۸۲). *جنگ ناهمتراز*، ترجمه عبدالمجید حیدری و محمد تمنائی، تهران، انتشارات سپاه پاسداران انقلاب اسلامی.

٥. مونکلر، هرفرید. (۱۳۸٤). *جنگ‌های نوین*، ترجمه حسین درگاهی، تهران، انتشارات سپاه پاسداران انقلاب اسلامی.

٦. دیوسالار، عبدالرسول؛ ولوی، محمدرضا؛ امیرخانی‌فراهانی، محمد و دانایی، محمدمهدی. (۱۳۸٥). *راهبردها و معماری کلان فرماندهی و کنترل جنگ اطلاعات* (جلد ۲). تهران، موسسه آموزشی و تحقیقاتی صنایع دفاعی.

۷. ضیایی پور، حمید. (۱۳۹۱). *جنگ نرم ۱(ویژه جنگ رایانه ای)*. تهران، انتشارات مرکز مطالعات و تحقیقات بین المللی ابرار معاصر.

8. Alvin, J., & Ronfeldt, D. (1997). *In Athena's camp: Preparing for conflict in the information age*. Rand corporation.
9. Heisbourg, F. L. (2002). Europe's Military Revolution. *Hampton Roads International Security Quarterly*, 27-31.
10. Dana, M. G. (2003). *Shock And Awe: America's 21st Century Maginot Line*. NAVAL WAR COLL NEWPORT RI JOINT MILITARY OPERATIONS DEPT.
11. Blaker, J. R., & Manning, R. A. (1997). *Understanding the revolution in military affairs: A guide to america's 21st century defense*. Progressive Policy Institute.
12. Cahill, T. P., Rozinov, K., & Mule, C. (2003, June). Cyber warfare peacekeeping. In *IEEE Systems, Man and Cybernetics SocietyInformation Assurance Workshop, 2003*. (pp. 100-106). IEEE.

1. Monitoring