مفهوم‌شناسیِ رویکرد تهاجمی به اطلاعات

احسان کیانی [1]
هادی تاجیک [2]

تاریخ دریافت: ۱۳۹۹/۰۷/۱۱ **تاریخ پذیرش نهایی: ۱۴۰۰/۰۶/۲۱**

نشریه علمی آفاق امنیت / سال چهاردهم / شماره پنجاه و یکم ـ تابستان۱۴۰۰ : ۹۵-۷۳

چکیده

در شرایطی که اهمیت نبردهای اطلاعاتی در منازعات بین‌المللی بر کسی پوشیده نیست، دست‌یابی به تعریفی نسبتاً دقیق از رویکرد تهاجمی به اطلاعات، می‌تواند تصمیم‌سازان امنیت ملی کشور را هم ازمنظر پدافندی ـ در شناسایی هجمه‌های اطلاعاتی ـ و هم ازمنظر آفندی ـ در طراحی راهبردهای تهاجمی ـ یاری کند. در راستای تولید ادبیات فارسی‌زبان درخصوص اطلاعات تهاجمی، این پژوهش برمبنای ارزیابی پژوهش‌های آشکار لاتین با روش توصیفی ـ تحلیلی برمبنای گردآوری کتابخانه‌ای، به تبیینی از مسأله تهاجم اطلاعاتی مبادرت می‌ورزد. ارزیابی تعاریف این رویکرد در منابع غربی نشان می‌دهد می‌توان تهاجم اطلاعاتی را، نوعی حمله پیش‌دستانه به چرخه اطلاعاتی منتج به تصمیم‌سازی دولت/سازمان‌های متحد، مؤتلف، رقیب یا متخاصم دانست که با هدف مدیریت ادراک و تغییر محاسبات آن، زمین بازی را مطابق منافع خودی طراحی می‌کند تا به مهار یا تغییر رفتار طرف مقابل بینجامد. در رویکرد تهاجمی به اطلاعات برای تغییر موازنه نیروها، لازم است نبض داده‌های کاربردی حریف در دست قراربگیرد تا بدین‌وسیله بتوان طراحی‌ها و برنامه‌ریزی‌های دشمن را تحت تأثیر قرارداده و حتی به آن‌ها مطابق منافع خودی، جهت داده شود.

واژگان کلیدی
تهاجم اطلاعاتی؛ برتری اطلاعاتی؛ آگاهی بر میدان؛ دانش مسلط.

۱. دانشجوی دکتری مطالعات منطقه، دانشگاه جامع امام حسین، تهران، ایران E1386k@gmail.com
۲. نویسنده مسئول: استادیار، دانشگاه جامع امام حسین(ع)، تهران، ایران Int.1358@yahoo.com

مقدمه

اهمیت اطلاعات[1] در نبردهای امنیتی، نظامی، سیاسی یا اقتصادی دولت‌ها در عصر کنونی بر کسی پوشیده نیست. در این منازعات آنکه دست برتر را در حوزه اطلاعاتی دارد، به‌وضوح احتمال بیشتری برای غلبه بر رقیب دارد. تفوق اطلاعاتی چه پیش و چه در هنگامه نبرد، سبب کاهش آسیب‌پذیری سیستم و پیشگیری از بروز تلفات جدی خواهد شد. اگر ابتدا برتری اطلاعاتی عمدتاً به گردآوری و کسب اطلاعات حساس و مهم مرتبط بود؛ اما اکنون نه‌لزوماً حجم اطلاعاتِ در دسترس، بلکه روش تحلیل و بهره‌برداری از آن و حتی ایجاد تغییر در اطلاعاتِ در دسترس رقیب نیز، اهمیت بسیاری یافته است.

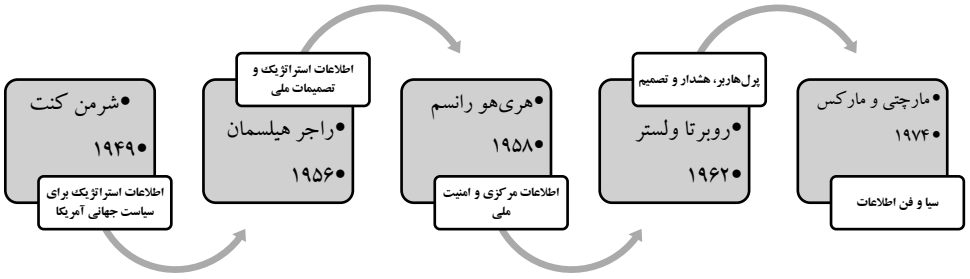
تاکنون پژوهش‌های بسیاری در حوزه پدافند اطلاعاتی مانند ضدجاسوسی، ضدتروریسم، ضدنفوذ و ضدفریب به رشته تحریر درآمده است، ولی در زمینه آفندی مبتنی بر رویکرد تهاجم اطلاعاتی[2]، ادبیات قابل‌توجهی به زبان فارسی تدوین نشده است. حال آنکه اقدام اطلاعاتی چه به‌مثابه یک اقدام پیش‌گیرانه یا به‌عنوان ضربه اول جهت پیش‌دستی در نبرد، می‌تواند موضع ساختار سیاسی را به‌نحو چشم‌گیری تقویت نماید. از جنبه پیش‌گیرانه، واردکردن ضربه‌های امنیتی به‌طرف مقابل، پیش از ورود به مواجهه سخت یا جهت اجتناب از چنین رویارویی، اهمیت بسیاری دارد. هم‌چنین می‌توان با طراحی اقدامات ایجابی در زمین بازی، ضربه اول را طوری وارد کرد که دشمن از حالت فعالانه خارج شده و توانایی مقابله جدی را از دست بدهد. به همین دلیل، پردازش جنبه‌های گوناگون تهاجم اطلاعاتی می‌تواند یاری‌گر سازمان‌ها و افسران اطلاعاتی باشد.

ضرورت این پژوهش در شرایط کنونی که کشور تحت تهاجم همه‌جانبه اقتصادی، اطلاعاتی، دیپلماتیک و حتی نظامی قرار گرفته، کاملاً مشهود است. تداوم این جنگِ ترکیبی، می‌تواند دستگاه‌های حوزه امنیت ملی را با چالش‌های جدی مواجه کند. این مسأله به‌ویژه مورد تأکید رهبر معظم انقلاب نیز قرار داشته که در این خصوص می‌فرمایند: «باید در این جنگ [اطلاعاتی] و در مقابل برنامه‌های جبهه مقابل ایستاد و برای غلبه‌بر دشمن، علاوه‌بر دفاع، باید برنامه تهاجم نیز داشت؛ به‌گونه‌ای که زمین بازی به‌وسیله دستگاه اطلاعاتی ما تعیین شود» (خامنه‌ای، ۱۳۹۷/۱۰/۲۹). از آنجا که این پژوهش، ماهیت اکتشافی دارد بنابراین فاقد فرضیه است.

1. Intelligence
2. Offensive Intelligence

روش پژوهش

مطالعات اطلاعات، ریشه در پژوهش‌های مرتبط با منازعات دیپلماتیک دارد، چنان‌که حتی آن‌را «زیررشته‌ای از روابط بین‌الملل» قلمداد کرده‌اند (علی‌خانی، ۱۵:۱۳۹۴). اگر با رویکرد فوکویی به مسأله بنگریم و توسعه یک دانش را با کارکرد آن، در حفظ و بسط قدرت هم‌بسته تلقی نماییم، توسعه مطالعات مربوط به امنیت ملی و دانش اطلاعاتی نیز به پس از جنگ جهانی دوم بازمی‌گردد که بخش مهمی از توفیق یا ناکامی دولت‌ها، به توان‌مندی اطلاعات نظامی آن‌ها مربوط بود؛ از غافلگیری بزرگ آمریکا در نبرد پرل‌هاربر توسط ژاپن تا شکست سهمگین نیروهای آلمان در سواحل نرماندی. بازخوانی این تجربه‌ها به‌ویژه با توجه به آغاز جنگ سرد، اهمیت فزون‌تری یافت؛ زیرا فعالیت‌های جاسوسی و ضدجاسوسی دو ابرقدرت هسته‌ای جهان در راستای مقابله با نفوذ یکدیگر، گسترش بیشتری پیدا کرد. دولت آمریکا نیز به تأسی از موفقیت‌های اطلاعاتی بریتانیا در جنگ جهانی دوم و در راستای تضعیف تهدید بالقوه اتحاد جماهیر شوروی، دو سال پس از پایان جنگ جهانی، «آژانس مرکزی اطلاعاتی آمریکا[1]» موسوم به سیا را در سال ۱۹۴۷ تأسیس کرد. به‌تبع این تحولات در حوزه قدرت سیاسی، اولین متون دانشی در حوزه اطلاعاتی نیز از سوی کارشناسان سی‌آی‌ای یا پژوهش‌گران مرتبط با این سازمان به‌رشته تحریر درآمد.



شکل ۱. اولین کتب منتشره در حوزه اطلاعات به تفکیک نویسنده و سال نشر (معاونت پژوهش و تولید علم، (ب)، ۱۳۹۵:٤٠).

تجربه‌های قلمی کارشناسانِ بازنشسته جامعه اطلاعاتی، به‌تدریج به انباشت دانش در

1. Central Intelligence Agency (CIA)

این زمینه منجر شد و به تأسیس «دانشگاه ملی اطلاعات[1]» در سال ۱۹۶۲ با حمایت آژانس اطلاعات دفاعی و آموزش رشته اطلاعات در مقاطع کارشناسی و کارشناسی ارشد انجامید (معاونت پژوهش و تولید علم، (ب)، ۱۳۹۵، ۴۰). عضویت افسران سابق جامعه اطلاعاتی آمریکا در هیأت‌های علمی این دانشگاه و هم‌چنین انتشار خاطرات و تجربیات‌شان در قالب مقالات یا مصاحبه‌های مطبوعاتی، در کنار فعالیت‌های دیگر اعضای دولت مانند کارمندان وزارت دفاع، به‌تدریج بر غنای دانش انباشته‌شده در زمینه اطلاعات افزود. با وجود موارد مذکور، یکی از مهم‌ترین خلأهایی که میان مطالعات اطلاعات با دیگر رشته‌های علوم انسانی هم‌چون جامعه‌شناسی و علوم سیاسی فاصله عمیقی ایجاد کرده و هم‌چنان آن‌را به‌مثابه یک زیررشته یا حداکثر میان‌رشته‌ای از تاریخ و سیاست در نوسان نگاه داشته، فقدان نظریه‌های جامع و کاملی است که هم هویت یک رشته علمی را در این حوزه تقویت نماید و هم مطالعات پژوهش‌گران و دانشجویان این رشته را به‌سمت‌وسویی روشن سوق دهد.تنوع نظام‌های سیاسی، گوناگونی سرویس‌ها، تفاوت منابع ازمنظر جنس و نوع دسترسی و میزان انتشار داده‌های مرتبط با موفقیت یا شکست عملیات‌ها را می‌توان مهم‌ترین موانع شکل‌گیری یک یا چند نظریه اطلاعاتی غنی و مورد اجماع دانست (علی‌خانی، ۸۷:۱۳۹۴). به‌تبع درباره «تهاجم اطلاعاتی» حتی در متون انگلیسی‌زبان نیز، ادبیات قابل توجهی در این خصوص یافت نمی‌شود. نمونه این امر را می‌توان در تفکیک موضوعی مقالات نشریه «اطلاعات و امنیت ملی[2]» ـ که از سال ۱۹۸۶ انتشارش را به‌صورت دوماه‌نامه آغاز کرده بود ـ مشاهده کرد.

جدول ۱. تفکیک موضوعی مقالات نشریه «اطلاعات و امنیت ملی» از ۱۹۸٦ تا ۲۰۱۱؛ (معاونت پژوهش و تولید علم، (ب)، ۵٤:۱۳۹۵)

موضوع	میزان	موضوع	میزان
تاریخچه و بیوگرافی	۲۲٪	پاسخ‌گویی	٦٪
جمع‌آوری اطلاعات	۱۹٪	سازمانی	٤٪
ضداطلاعات	۱۰٪	آژانس‌های غیرآمریکایی	٤٪
تحلیل	۹٪	اطلاعات نظامی	٤٪
نظریه/روش	۸٪	انتشار	٤٪
اقدام پنهان	۷٪	تخیلی	۳٪

1. National Intelligence University
2. Intelligence and National Security

گرچه هیچ‌یک از این عناوین را نمی‌توان تحت‌عنوان «تهاجم اطلاعاتی» تفسیر کرد؛ ولی مجموع کار مطالعاتی در حوزه‌های اقدام پنهان و اطلاعات نظامی که احتمال قرابت بیشتری با «تهاجم اطلاعاتی» دارند، نشان می‌دهد حداقل در منابع آشکار غربی نیز نمی‌توان تصویر روشنی از آنچه تحت این عنوان، به‌کاربرده می‌شود یافت؛ بنابراین در این پژوهش تلاش می‌شود تا برمبنای یافته‌های موجود در منابع آشکار داخلی و خارجی، به مفهومی نزدیک به آن دست یافت. با این حال لازم به ذکر است که مهم‌ترین مسأله این پژوهش، محدودیت دسترسی به داده‌های طبقه‌بندی‌شده بوده است. آنچه از منابع لاتین موردارزیابی قرارگرفته، مواردی است که در جست‌وجوی آشکار یافت‌شده، کمااینکه ممکن است در پژوهش‌های درون‌سازمانی جامعه اطلاعاتی جمهوری اسلامی ایران نیز فعالیت‌هایی در این‌خصوص انجام شده باشد که طبعاً قابل دسترسی نبوده‌اند. با این حال سعی شده با روش توصیفی ـ تحلیلی برمبنای گردآوری کتابخانه‌ای از بررسی موارد آشکار، روندی مشخص استخراج شود. در این پژوهش ابتدا تعریفی از مفهوم اطلاعات و نبرد اطلاعاتی ارائه می‌شود، سپس برمبنای آن، رویکرد تهاجمی به اطلاعات موردارزیابی قرارمی‌گیرد.

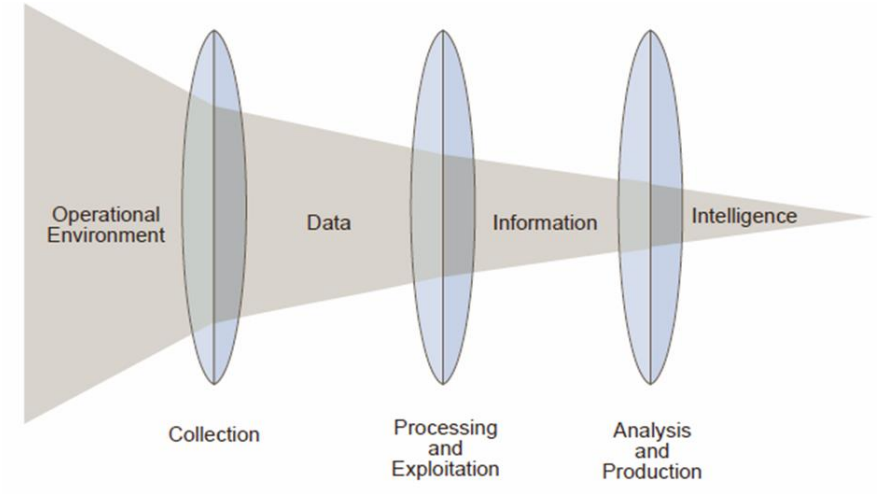
پیشینه پژوهش

در متون و پژوهش‌های فارسی منتشره در منابع آشکار، عبارت «تهاجم اطلاعاتی» به‌مثابه یک مفهوم رویکردی مشاهده نشده است. در برخی مقالات و آثار پژوهشی، تهاجم اطلاعاتی به‌معنای جنگ اطلاعاتی یا نبرد اطلاعاتی به‌کاررفته که نه به‌عنوان «قیدی» بر نوع اقدام اطلاعاتی، بلکه به‌گونه «صفت» بر آن بار شده است. برخی جنگ اطلاعاتی را اقدامی مبتنی‌بر زیرساخت‌های فناورانه دانسته‌اند که داشته‌های اطلاعاتی حریف را تحت تأثیر قرار می‌دهد (رشیدزاده، ۵۰:۱۳۸۵). برخی دیگر نبرد اطلاعاتی را دست‌یابی به برتری در منازعات سیاسی، اقتصادی یا نظامی در عرصه بین‌المللی در عصر پیشرفت‌های تکنولوژیک و فناوری اطلاعات خوانده‌اند (فضائلی، ۶۵:۱۳۸۷). این پژوهش‌گران متأثر از رشد بی‌سابقه کارکرد فضای مجازی و کاربران شبکه‌های اجتماعی در میانه دهه ۱۳۸۰ در ایران، اطلاعات را در بستر فناوری اطلاعات فهم نموده‌اند. در این بین افرادی که آشنایی بیشتری با مفهوم اطلاعات در حوزه امنیت ملی داشته‌اند، تهاجم اطلاعاتی را صرف هر نوع اقدام آفندی در حوزه اطلاعات به‌خصوص پس از جنگ سرد قلمداد کرده‌اند (صابرفرد، ۹۳:۱۳۹۱). این تعاریف نشان‌گر آن است که تعبیر تهاجم اطلاعاتی، به مفهومی که عملیات اطلاعاتی را مقید به نوع خاصی از اقدام نماید، هنوز در میان پژوهش‌گران

کشورمان تثبیت نشده و در ابتدای راه دریافت و بسط آن هستیم. به همین دلیل، رجوع به برخی متون پژوهشی و تخصصی انگلیسی‌زبان در حوزه دانش و تجربه نهادهای نظامی و امنیتی شاید راه‌گشا باشد.

جنگ اطلاعاتی

بعضاً در برگردانِ فارسیِ سهِ واژهِ لاتینِ Data، Information و Intelligence، از تعبیر اطلاعات استفاده می‌شود. حال آنکه واژه اول، مشاهدات و تجربیات اولیه‌ای است که پس از دسته‌بندی و منطق درونی به مورد دوم بدل می‌شود و نهایتاً پس از ارزیابی و تجزیه و تحلیل دقیق به knowledge تبدیل می‌شوند. واژه سوم درواقع برساخت سازمانی و تشکیلاتی آن در عرصه نظامی و امنیتی است (والتز، ۱۶:۱۳۸۷).



شکل ۲. فرآیند تبدیل شواهد و داده به اطلاعات (CJCS, 2013:2).

اولین نقش اطلاعات در نبردهای نظامی نمایان شد. «سان تزو» استراتژیست مشهور چین باستان و نویسنده اثر «هنر جنگ»، گردآوری اطلاعات را اقدامی پنهان با هدف غافلگیری دشمن قلمداد می‌کند (علی‌خانی، ۷۷:۱۳۹۴). او معتقد است اطلاعات، عاملی اساسی در کاهش نااطمینانی طرف خودی و افزایش تردید دشمن است؛ چیزی که امروزه عدم قطعیت خوانده می‌شود (علی‌خانی، ۱۴۱:۱۳۹۴). نکته‌ای که «کلازویتس» استراتژیست نظامی آلمانی نیز به آن اشاره و غافلگیری را عنصری ضروری برای پیروزی بر دشمن تلقی نموده که نشان‌گر اهمیت برتری اطلاعاتی در منازعات نظامی دوران میانه اروپاست (علی‌خانی، ۱۲۳:۱۳۹۴). با این حال، گرچه سان تزو بر کارکردهای اطلاعاتی مانند فریب، ضداطلاعات و کسب آگاهی از وضعیت درونی دشمن تأکید داشت، کلازویتس

در کارآمدی قطعی اطلاعات در جنگ، تردید ایجاد کرد و هم‌چنان بـر تجربـه فرمانـدهان، افزایش کیفیت و کمّیت نیروها تمرکز کرد (Bishop, 2003, 114).

با وقوع جنگ‌های جهانی، افسران امنیتـی غربـی سـعی کردنـد تعـاریف دقیـق‌تـری از اطلاعات ارائه دهند. «دیوید کان» مورخ برجسته اطلاعات نظـامی آمریکـا، آن‌را جـایگزین فقدان نیرو و توان رزمی خوانده است (علی‌خانی، ۷۸:۱۳۹۴). چنان‌چه «یولین وایـت‌هـد» افسر نیروی هوایی آمریکا معتقد بود «سلاح اطلاعات در ترکیبی با سـلاح‌هـای کلاسـیک، به‌منزله یک سلاح پیشرو برای کورکردن چشم دشمن پیش از انجام عملیات به‌کـار گرفتـه می‌شود» (والتز، ۲۷:۱۳۸۷). با آغاز جنگ سرد، به‌تدریج «اطلاعات در جنگ» جای خود را به «اطلاعات به‌مثابه جنگ» داد. به بیان دیگر، این بار اطلاعـات، خـود سـوژه نبـرد بـود و رقیبان، آن‌را هدف قرار می‌دادند. با تشکیل و توسعه سازمان‌های اطلاعاتی، «شرمن کنـت» ـ افسر اطلاعاتی آمریکا ـ آن‌را «ایجاد آگاهی نسبت به فعالیت تشکیلاتی در راستای اهداف امنیتی» و «مایکل هرمن» افسر اطلاعاتی سـابق بریتانیـا، آن‌را «شـکلی از قـدرت دولـت» دانستند (علی‌خانی، ۱۶:۱۳۹۴). «جیمز دردریان» مدیر مرکز مطالعات امنیـت بـین‌الملـل دانشگاه سیدنی نیز اطلاعات را «ادامه جنگ به روش اقدام پنهان» توصـیف کـرد (معاونـت پژوهش و تولید علـم، (ب)، ۹۲:۱۳۹۵) و در یکـی از جدیـدترین تعـاریف، دکتـر «مایکـل وارنر» ـ استادیار دانشگاه جان‌هاپکینز، افسر اطلاعاتی سابق امنیت سایبری آمریکـا و عضـو فعلی هیئت تحریریه نشریه «اطلاعات و امنیت ملـی» ـ اطلاعـات را «شـامل فعالیـت‌هـا و اخبار پنهان لازم برای تصمیم‌گیری ملی» تعریف می‌کند (علی‌خانی، ۷۶:۱۳۹۴). سیر ایـن تعاریف نشان می‌دهد به‌تدریج با شکل‌گیری اقتضائات جدید، تعاریف اطلاعات بـا دو تغییـر مواجه شد؛ اول آنکه از ابعاد نظامی به ابعاد سیاسی ـ امنیتی نیز تسری یافت و دیگر اینکـه از سطح خارجی به سطح داخلی گسترش پیدا کرد؛ بنابراین اطلاعـات را مـی‌تـوان چنـین تعریف کرد:

«هر گونه داده پردازش‌شده از منابع آشکار یا پنهان که دولت، برای تصمیم‌گیری جهت نیل به منافع ملی و حفظ امنیت ملی بدان نیازمند است.»

تعریف فوق، تفاوت آن با اطلاعـات بـه‌معنـایی کـه از آن تحـت واژه Information یـاد می‌شود را به‌خوبی نشان می‌دهد. Information به داده‌هـایی اطـلاق مـی‌شـود کـه گرچـه پردازش شده‌اند ولی

۱. از منابع صرفاً آشکار دریافت می‌شوند؛
۲. برآورد یا تحلیلی نسبت به حوزه امنیت ملی ارائه نمی‌دهند و
۳. برای تصمیم‌گیری یا تصمیم‌سازی مقام‌های دولت، الزامی نیستند.

با توسعه و گسترش فناوری‌های اطلاعات، به‌تدریج دگرگونی‌های وسیعی در منازعات سیاسی و امنیتی پدید آمد. این تغییرات، هم اهداف و هم تسلیحات نبردهای مرسوم را از انحصار زیرساخت‌های فیزیکی خارج کرد. چنان‌چه ایده موج سوم تافلر در ۱۹۸۰ مطرح می‌سازد، جهان با عبور از دو عصر کشاورزی و صنعتی، وارد عصر اطلاعات شده که طی آن اطلاعات، عامل اصلی تولید ثروت و قدرت بوده و محور اصلی منازعات از ایدئولوژی و اقتصاد، به اطلاعات تغییر خواهد کرد (والتز، ۳۴:۱۳۸۷). تمرکز بر نبرد اطلاعات به‌خصوص از این منظر اهمیت یافت که معطوف به بروز منازعات کلاسیک در ابعاد فیزیکال نیست و اتفاقاً در دوران صلح ضرورت بیشتری می‌یابد؛ زیرا علاوه‌بر کارکرد نبرد اطلاعاتی در دوران جنگ‌های نظامی، معمولاً در شرایطی که توجیه مناسبی برای ورود به نبرد سخت‌افزاری وجود ندارد نیز از فرآیندهای متناظر با جنگ اطلاعات استفاده می‌شود. نمونه شاخص آن، جنگ نرم آمریکا علیه شوروی در دوران جنگ سرد و پروژه‌هایی مانند جنگ ستارگان است که در ابعاد نظامی، اقتصادی، سیاسی و فرهنگی، ضربات سهمگینی بر امنیت نرم اتحاد جماهیر شوروی واردکرد. چنان‌چه طبق تعریف عملیاتی وزارت دفاع آمریکا، جنگ اطلاعاتی به‌معنای اجرای یک عملیات اطلاعاتی علیه دشمن معیّنی در شرایط جنگ یا بحران است (والتز، ۲۳۹:۱۳۸۷).

دسته‌بندی‌های مختلفی از انواع جنگ اطلاعاتی ارائه شده است. «دیوید رونفلت» در ۱۹۹۳ آن‌را به سه دسته اصلی تقسیم می‌کند:

جدول ۲. انواع جنگ اطلاعات طبق ایده‌پردازی دیوید رونفلت (والتز، ۳۸:۱۳۸۷).

نوع	هدف	روش
جنگ شبکه‌ای	مدیریت درک جامعه کشور هدف	کنترل اطلاعات ازطریق ارتباطات شبکه‌شده
جنگ سیاستی	تأثیر بر تصمیم‌های رهبری دولت هدف	اثرگذاری بر معیارهای تصمیم‌های سیاسی و اقتصادی
جنگ فرماندهی	هدایت عملیات علیه اهداف نظامی	فریب، عملیات روانی و جنگ الکترونیک

در جنگ شبکه‌ای، مهاجم ازطریق ایفای نقش در شبکه‌های ارتباطی عمومی اعم از رادیو و تلویزیون، مطبوعات یا فضای مجازی، درصدد تغییر درک توده‌های جمعیت یک دولت نسبت به سوژه‌ای خاص مطابق با منافع خودی برمی‌آید. به‌همین سبب جنگ اطلاعات در قالب نبردی در شبکه‌های حاوی اطلاعات نمود می‌یابد. انتشار اخبار و

تحلیل‌های خاص، جلوگیری از نشر داده‌های مؤثر یا تلفیقی از این دو، ازجمله ابزارهای این نبرد محسوب می‌شوند. در جنگ سیاستی، مهاجم تلاش می‌کند تا بر اطلاعات مؤثر بر تصمیم‌گیری‌ها و سیاست‌گذاری‌های نخبگان دولت هدف تأثیر گذاشته و به تغییر محاسبات آنان مبادرت ورزد. البته یکی از مقدمات این اثرگذاری در ساخت‌های سیاسی مردم‌سالار، می‌تواند توفیق در جنگ شبکه‌ای قلمداد شود. امری که گرچه بلندمدت‌تر و نسبتاً دشوارتر است؛ ولی اثراتی عمیق‌تر و پایدارتر برجای‌خواهدگذاشت. نوع سوم دسته‌بندی رونفلت، نبردی بر سر کنترل محیط یک عملیات نظامی است. این تقسیم‌بندی برمبنای اهداف نبرد صورت‌گرفته است؛ ولی نمی‌توان هم‌پوشانی برخی روش‌ها را در اهداف دیگر ـ برای مثال کاربرد فریب در تأثیر بر تصمیم‌سازی‌های نخبگان دولت هدف یا کاربرد عملیات روانی علیه جامعه هدف ـ را منتفی دانست.

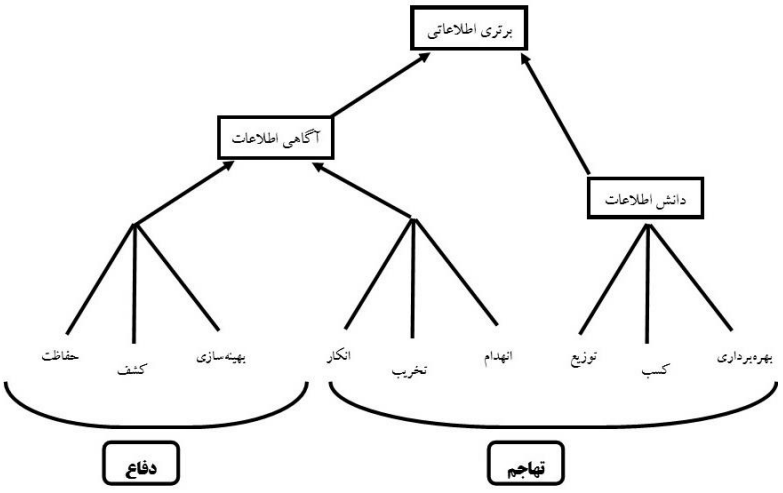
وبن شوارتو در ۱۹۹۴ برمبنای هدف، دسته‌بندی دیگری ارائه داده که شامل اشخاص عمومی، شرکت‌های خصوصی و دولت‌های ملی است (والتز، ۴۳:۱۳۸۷). به‌نظر می‌رسد این تقسیم‌بندی بیشتر با رهیافت اقتصادی تدوین شده و برمبنای آنکه مهاجم با ورود به شبکه اطلاعات و دخل‌وتصرف در ورودی‌های مؤثر بر تصمیمات، منافع کدامین بخش از جامعه ـ به‌خصوص در ساخت‌های سیاسی سرمایه‌دارانه ـ را متضرر سازد، به سه دسته تقسیم شده‌اند. مارتین لیبیکی در ۱۹۹۵ تقسیم‌بندی دیگری ارائه داده که بیشتر بر روش‌های جنگ اطلاعات متمرکز است: جنگ الکترونیک، جنگ روانی، جنگ کنترل و فرماندهی، جنگ هکر و جنگ سایبری (والتز، ۴۰:۱۳۸۷). مؤلف در این تقسیم‌بندی، اهداف نظامی و امنیتی را مدنظر قرار داده است. رابرت استیل در ۱۹۹۲ ماتریسی درخصوص انواع جنگ اطلاعات ارائه داد که شامل دو مؤلفه زمان و ابزار است.

فناوری	زمان: کوتاه مدت	زمان: بلندمدت
بالا	هدف‌گیری دقیق قلمرو فیزیکی	هدف‌گیری پایگاه داده
پایین	هدف‌گیری تصادفی قلمرو فیزیکی	هدف‌گیری ایدئولوژیک توده مردم

شکل ۳. انواع جنگ اطلاعات در ایده‌پردازی استیل (والتز، ۴۲:۱۳۸۷).

نبردهای اطلاعات در بازه بلندمدت و با فناوری بالا، نبردی بر سر کنترل و فرماندهی اطلاعات در فضای سایبر توصیف شده که اساس قدرت را، تسلط بر دانش قلمداد می‌کند.

فناوری بالا در بازه کوتاه‌مدت به درگیری‌های با شدت متوسط به بالا می‌انجامد که قصد تسلط بر حوزه فیزیکی قدرت به‌ویژه پول را در عصر مدرن در پی دارد. فناوری‌های ضعیف‌تر در بلندمدت عمدتاً ازمنظر استیل، توسط گروه‌های ایدئولوژیک برای جنگ رسانه‌ای علیه جوامع توده‌ای به‌کارگرفته‌می‌شود و نبردهای اطلاعاتی با فناوری پایین و در بازه کوتاه‌مدت به درگیری‌های کم‌شدت با اهداف فیزیکی ختم می‌شود. در تداوم تلاش برای تبیینی دقیق‌تر از نبرد اطلاعاتی که می‌توان آن را جمع‌بندی کامل‌تری از مباحث پیشین تلقی کرد، وزارت دفاع آمریکا در سال ۱۹۹۵ تعریفی از جنگ اطلاعات عرضه داشت که ورای روش، هدف کلی آن را در هر دو رویکرد تدافعی و تهاجمی، برتری اطلاعاتی عنوان نمود.



شکل ٤. جنگ اطلاعات طبق تعریف وزارت دفاع آمریکا (والتز، ٤٥:١٣٨٧).

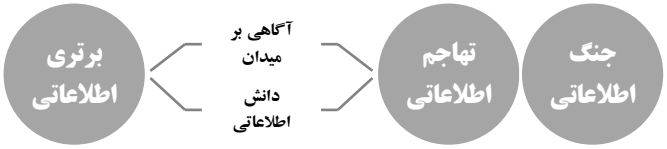
بنابراین نبرد اطلاعاتی، فرآیند بهره‌برداری از اطلاعات در منازعات سیاسی، دیپلماتیک، نظامی، امنیتی یا اقتصادی محسوب می‌شود که به برتری اطلاعاتی منجر گردد. بخشی از فرآیند کسب برتری اطلاعاتی، دو رویکردِ هم‌زمانِ حمله به سیستم اطلاعاتی دشمن و مقابله با حملات به سیستم خودی است. حفاظت از محتوا و پردازش اطلاعات، کشف اقدامات ضداطلاعاتی، بهینه‌سازی سیستم‌های ذخیره و تبادل اطلاعات، مهم‌ترین وجوه رویکرد دفاعی در این تعریف است. در عین حال، بخشی از رویکرد تهاجمی با انکار اطلاعات سبب گمراهی حریف شده یا با حملاتی به تخریب یا انهدام سیستم رقیب دست یازیده و دسترس‌پذیری، محرمانگی یا یکپارچگی اطلاعات برای او را مختل می‌سازد و هر

دو به آگاهی مسلط بر میدان نبرد[1] در ابعاد مختلف سیاسی، نظامی و امنیتی و درنتیجه، به برتری اطلاعاتی می‌انجامد. بخشی از رویکرد تهاجمی در این تعریف که به‌نوعی بازآرایی همان چرخه اطلاعات است، به جمع‌آوری اطلاعات از محیط ازجمله سیستم‌های رقیب و متخاصم، پردازش و توزیع آن در جبهه خودی مربوط می‌شود که با کسب دانش مسلط بر میدان نبرد[2]، به برتری اطلاعاتی منجر می‌شود. در این فرآیند، کسب آگاهی مقدمه‌ای بر کسب دانش قلمداد می‌شود. در شرایطی که نتوان با حملات اطلاعاتی دشمن مقابله کرده و از محیط ازجمله قلمروی تحت‌سلطه رقیب، اطلاعات ارزشمندی کسب کرد، دست‌یابی به دانشِ برآمده از داده‌های اکتسابی نیز اگر نه غیرممکن، ولی بسیار دشوار خواهد بود. والتز در «عملیات و اصول جنگ اطلاعات» مزایای برتری اطلاعاتی را چنین برمی‌شمارد (والتز، ۱۳۸۷:۱۶۱):

- **آماده‌سازی میدان نبرد:** تهیه اطلاعات خاص از میدان منازعه شامل ابعاد فیزیکی، سیاسی، شبکه ارتباطی و مانند آن، که با کاوش فعال و پیمایش دقیق اهداف معین رخ می‌دهد. به‌تبع آسیب‌پذیری‌ها و محدودیت‌های دشمن تعیین شده و واکنش‌های بالقوه تهاجمی‌اش پیش‌بینی می‌شود.
- **تحلیل میدان نبرد:** مشاهده مستمر میدان نبرد و تحلیل مشاهدات جمع‌آوری‌شده به درک تفصیلی از وضعیت‌های پویا و متغیر و استنتاج الگوهای رفتاری در دوره‌های زمانی متفاوت می‌انجامد.
- **تجسم میدان نبرد:** طی این فرآیند، رهبریِ جبههِ خودی درک روشنی از وضعیت جاری در ارتباط با دشمن و محیط کسب می‌کند. وضعیت پایانی مطلوب را ترسیم نموده و توالی اقداماتی را که از وضعیت کنونی به نقطه مطلوب می‌رسد، تعیین می‌نماید.
- **توزیع آگاهی میدان نبرد:** بخش‌هایی از آگاهی مکتسبه به مشترکین و مشتریان مناسب در زمان‌های مقتضی و در قالب مأموریتی معین، توزیع می‌شود.

بنابراین رویکرد تهاجمی در جنگ اطلاعات، بر دو هدف کسب آگاهی و دانش مسلط بر حوزه مورد منازعه و درنتیجه برتری اطلاعاتی در این خصوص متمرکز است. این برتری اطلاعاتی، نقش اساسی در تحمیل زمین بازی به حریف و تعیین مؤلفه‌های منازعه برمبنای مطلوبیت‌های بلوک قوی‌تر اطلاعاتی، ایفا خواهد کرد.

1. Dominate Battlespace Awareness
2. Dominate Battlespace Knowledge



شکل ۵. فرایند کسب برتری اطلاعاتی در رویکرد تهاجم اطلاعاتی.

تهاجم اطلاعاتی

توجه به این نکته لازم است که در مواردی که تهاجم اطلاعاتی یا نبرد اطلاعاتی به‌کاررفته، منظور از اطلاعات، Information می‌باشد که در فضای سایبر، شبکه‌های اجتماعی و امنیت فناوری‌های ارتباطات کارکرد دارد. دلیل این امر آن است که با پایان جنگ سرد، کارشناسان امنیتی و نظامی ایالات متحده، دایره رصد نقاط تهدید را هم از حیث جغرافیای سیاسی به فراتر از بلوک شرق توسعه دادند و هم از جنبه مفهومی، موضوعات جدیدی به آن افزودند. ازجمله تهدیدات جدی در سال‌های پس از جنگ سرد، مبحث امنیت سایبرسی دولت آمریکا بود. به‌همین‌جهت کارشناسان و پژوهشگران حوزه فناوری اطلاعات و امنیت سایبر در ارتش و دیگر ارگان‌های امنیتی، عمدتاً ازمنظر سلبی نسبت به چگونگی مقابله با تهاجم گروه‌های فروملی یا فراملیِ مخالف هژمونی آمریکا، در بستر فناوری اطلاعات و احتمال سوءاستفاده گروه‌های تروریستی از فضای شبکه‌های اجتماعی و بستر تحت وب، به تبیین تهاجم اطلاعاتی پرداختند. ازجمله زمینه‌هایی که حساسیت جامعه اطلاعاتی و ارگان‌های دفاعی غرب و به‌خصوص آمریکا را نسبت به مسأله تهاجم اطلاعاتی در بستر سایبری برانگیخت، می‌توان به اولین حملات عمومی سایبری در سال‌های پایانی دهه ۱۹۸۰ مانند انتشار ویروس اسب تروا[1] در ۱۹۸۹ یا حمله‌ای سایبری از مبدأ هلند به ۳۴ نقطه در ایالات متحده از آوریل ۱۹۹۰ تا مِی ۱۹۹۱ اشاره کرد (Hirschland, 2001, 1).

دکتر «جرج استین» مدیر وقت مرکز مطالعات عملیات فضای مجازی دانشگاه نیروی هوایی آمریکا در مقاله «تهاجم اطلاعاتی: نبرد اطلاعاتی در ۲۰۲۵» به پیش‌بینی امنیت سایبری دولت آمریکا در قرن بیست‌ویکم پرداخته است. وی رویکرد تهاجمی در اطلاعات را نوعی برتری اطلاعاتی قلمداد کرده بود که در بستر فناوری اطلاعات، «به اختلال در

1. Trojan

فرآیند شناختی هدف منجر می‌شود« (Stein, 1996, 7). این تعریف از تهاجم، نبردی به‌وسیله داده‌ها و به پشتوانه اطلاعاتی، با هدف ضربه‌زدن به امنیت نرم جامعه هدف است. حال آنکه امر اطلاعات، حداقل در مبانی کلاسیک، عمدتاً نخبگان عرصه قدرت را هدف قرار می‌دهد. به تعبیر دیگر، آنچه استین تحت‌عنوان تهاجم اطلاعاتی تبیین نمود، تا حدی می‌تواند به آنچه در همان سال‌ها در ایران از آن تحت عنوان «تهاجم فرهنگی» یاد می‌شد، نزدیک بوده باشد. با این تفاوت که استین صرفاً به تعاریف نظری بسنده نکرده و زیرساخت فنی تهاجم را رشد تکنولوژی‌های الکترونیک و ارتباطات شبکه‌های اینترنتی قلمداد کرده بود.

گسترش کمّی و کیفی کاربران رایانه در آمریکا به‌واسطه انتشار عمومی «ویندوز ۹۸» ازسوی شرکت مایکروسافت در سال ۱۹۹۹، ازجمله دلایلی بود که کارشناسان حوزه دفاعی و امنیتی ایالات متحده را نسبت به امنیت سایبر و هجوم اطلاعاتی گروه‌های ضدهژمون به فرآیند استدلالی گروه‌های مرجع در آمریکا، حساس‌تر کرد و به مرور، ابعاد امنیتی تهاجم اطلاعاتی در بستر سایبری، اهمیت بیشتری یافت. در همین راستا دکتر «مارتین لیبیسکی» مدرس مطالعات امنیت سایبر در دانشکده نیروی دریایی آمریکا و از پژوهش‌گران مؤسسه رَند[1]، در فصل پایانی کتاب «ارزیابی راهبردی: تغییر نقش اطلاعات در جنگ» که به تبیین تأثیر فناوری‌های اطلاعاتی بر نبردهای نظامی پرداخته، تهاجم اطلاعاتی را **ضربه مخفیانه به نخبگان** دانسته است (Libicki, 1999, 450). «پائول ژاویدنیاک» مدیربرنامه جنگ اطلاعاتی شرکت لوگیسون[2] که در زمینه ارائه خدمات نرم‌افزاری و فناوری اطلاعات به ارتش و وزارت دفاع آمریکا فعالیت دارد، طی مقاله «دست‌یابی به تاب‌آوری اطلاعاتی» به تبیین چگونگی مقابله با تهاجم سایبری می‌پردازد. این مقاله نیز تبیینی از تهاجم اطلاعاتی ارائه نمی‌دهد ولی برای مقابله، تاکتیک «دفاع از عمق» را پیشنهاد می‌دهد؛ بدین‌معنا که به‌جای رویکرد واکنشی تشخیص و مقابله با تهاجم، در پی ارزیابی و سپس اقدام پیش‌دستانه در عمق راهبردی فراتر از مرزهای سیستم باشیم (Zavidniak, 1999, 8)؛ بنابراین مشخص می‌شود تهاجم اطلاعاتی، **حمله‌ای به درون سیستم** قلمداد می‌شود.

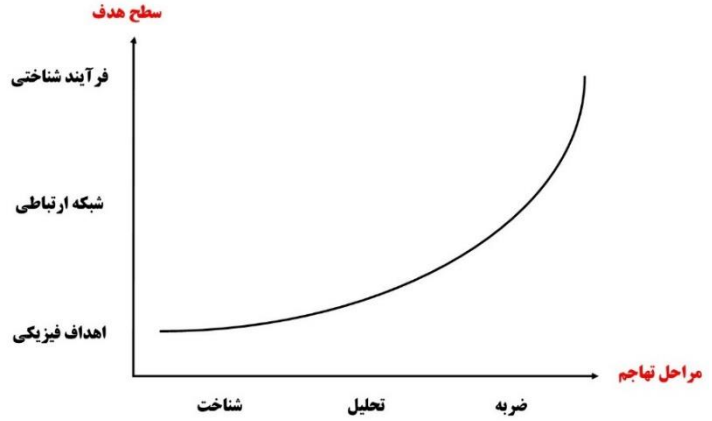
«دوروتی‌الیزابت دنینگ» محقق برجسته امنیت اطلاعات دانشگاه جرج‌تاون و استاد دانشگاه نیروی دریایی آمریکا نیز در ۱۹۹۹ کتابی تحت عنوان «جنگ اطلاعات و امنیت» متناظر به امنیت سایبری منتشر نمود. وی بهره‌مندی آمریکا از ابزارهای اطلاع‌رسانی در

1. Rand
2. Logicon

جنگ خلیج فارس را از مهم‌ترین نمونه‌های جنگ اطلاعات در دوران معاصر قلمداد کرده و بر نقش غیرقابل انکار عملیات روانی در پیروزی نیروی آمریکایی بر ارتش بعث عراق صحه می‌گذارد (دنینگ، ۵:۱۳۸۳). وی جنگ اطلاعاتی را عملیاتی با «حاصل‌جمع صفر» می‌داند که مخازن، حاملان، حس‌گرها، ضبط‌کننده‌ها یا پردازشگرهای اطلاعاتی را هدف قرار می‌دهد تا **محرمانگی، جامعیت یا دسترس‌پذیری اطلاعات** مهاجم را افزایش و آن‌را برای طرف مقابل کاهش دهد (دنینگ، ۲۳:۱۳۸۳). او جاسوسی، سرقت، نفوذ، عملیات روانی و فریب را ازجمله انواع جنگ اطلاعات تهاجمی می‌داند (دنینگ، ۳۸:۱۳۸۳).

با تبیین نخبگان درون ساختار قدرت سیاسی به‌عنوان مخاطب اصلی تهاجم اطلاعاتی، هدف این عملیات در آثار بعدی روشن‌تر شد؛ تأثیر بر تصمیم. «دونالد ولز» سرهنگ بازنشسته ارتش آمریکا، مدرس فناوری اطلاعات و مدیر امنیت اطلاعات دانشگاه پنسیلوانیا در مقاله «حمله متقابل، عملیات تهاجمی در نبرد اطلاعاتی» به بررسی ویژگی‌های نبرد با دشمنان آمریکا در بستر سایبری پرداخته و مؤلفه رویکرد تهاجمی را **سلب ابتکار عمل دشمن** تلقی نمود (Welch, 1999:50). دکتر «الکساندر وودکوک» استاد دانشگاه دفاع ملی استکهلم نیز در مقاله «پشتیبانی عملیات اطلاعاتی از تعامل نظامی مدنی»، دریافت خود را تهاجم اطلاعاتی، **نفوذ بر تصمیم‌گیران انسانی** بیان کرد (Woodcock, 1999:172). سپس مثال‌هایی از تهاجم اطلاعاتی در سه سطح راهبردی، عملیاتی و تاکتیکی مطرح می‌کند. مثلاً ایجاد بازدارندگی (مثال راهبردی)، فریب دشمن (مثال عملیاتی) و اخلال در پدافند هوایی (مثال تاکتیکی)، نمونه‌هایی از کاربرد تهاجم اطلاعاتی هستند (Woodcock, 1999:176).

«اِد والتز» مسئول بخش نوآوری‌های مرکز تکنیک‌های دفاعی‌اطلاعاتی وابسته به وزارت دفاع آمریکا که از مراکز پشتیبان جامعه اطلاعاتی و امنیتی ایالات متحده در حوزه امنیت شبکه‌های اجتماعی و فضای مجازی است، در «ادغام داده‌ها در عملیات‌های دفاعی و تهاجمی اطلاعاتی، «مسأله تهاجم ازطریق داده‌ها و اطلاعات» را موردبررسی قرارداد. به‌نظر او، این تهاجم با هدف اختلال در شبکه اطلاعاتی حریف در سه حوزه زیرساخت‌های فیزیکی، فضای سایبری و فرآیند شناختی صورت می‌گیرد. ازمنظر او، خطرناک‌ترین و مهم‌ترین هدف تهاجم اطلاعاتی، سومین لایه یعنی تأثیرگذاری بر تصمیم‌سازی رهبران جوامع و جهت‌دهی به الگوهای شناختی آن‌ها از عدم قطعیت‌ها، روندها و ریسک‌های احتمالی است؛ به‌نحوی که به **پذیرش مطلوبیت‌های مهاجم به‌مثابه منافع خودی** بینجامد(Waltz, 2000:5). شکل زیر، فرآیند تهاجم را ازمنظر والتز در این مقاله، ترسیم می‌کند.



شکل ٦. فرآیند اثرگذاری تهاجم اطلاعاتی در مدل والتز (Waltz, 2000:12).

شکل ۶ را می‌توان با مثالی تبیین کرد. در یک عملیات نظامی، نیروی مهاجم ابتدا سطح اهداف فیزیکی مانند تجهیزات، نیروی انسانی و محیط جغرافیایی را رصد می‌کند. در همین سطح نیز می‌تواند پس از تحلیل موقعیت مبنی‌بر نقاط ضعف و قوت خود و فرصت‌ها و تهدیدهای محیطی، ضرباتی را به قوای تسلیحاتی دشمن وارد نماید. درعین‌حال می‌تواند به سطح شبکه‌های ارتباطی دشمن نفوذ کرده و با تاکتیک‌هایی مانند جعل یا انکار اطلاعات، آسیب‌پذیری دشمن و طرح‌های پدافندی یا آفندی، او را نسبت به خود متأثر سازد؛ ولی سطح بسیار مؤثری که از تقریب اطمینان‌بخشی بالایی برخوردار است، آن است که فرآیند درک فرماندهان عالی‌رتبه دشمن در میدان نبرد را تحت‌تأثیر قراردهد. ابتدا با شناخت روحیات، موقعیت‌ها، تجارب و ایده‌های احتمالی آن‌ها و سپس تحلیل این موارد، می‌تواند ضربه‌ای به مراتب کارآتر از اهداف فیزیکی یا حتی شبکه نمادهای ارتباطی به او وارد نماید. اینکه چشم‌انداز آن فرماندهان از نبرد چنان متأثر شود که طرح مطلوب نیروی مهاجم را بدون نیاز به درگیری آشکار، به‌مثابه برنامه‌ریزی خودی به‌اجرا درآورند و این، سطح ضربه را عمیق‌تر و آثار آن‌را بلندمدت‌تر خواهد ساخت (والتز، ۳۴۹:۱۳۸۷).

والتز کمی پیش‌تر در فصلی از کتاب «عملیات و اصول جنگ اطلاعات» ــ منتشره در ۱۹۹۸ ـ تحت عنوان «عملیات اطلاعات تهاجمی» نیز به این مفهوم پرداخت. وی در ابتدای این فصل مدعی می‌شود که عملیات اطلاعات تهاجمی را می‌توان به طُرُق قانونی یا غیرقانونی، اخلاقی یا غیراخلاقی و به بیان دیگری مجاز یا غیرمجاز اجرا کرد. وی در ادامه، انگیزه‌اش از تبیین رویکرد تهاجمی را درک زمینه حملات دشمنان آمریکا عنوان نمود

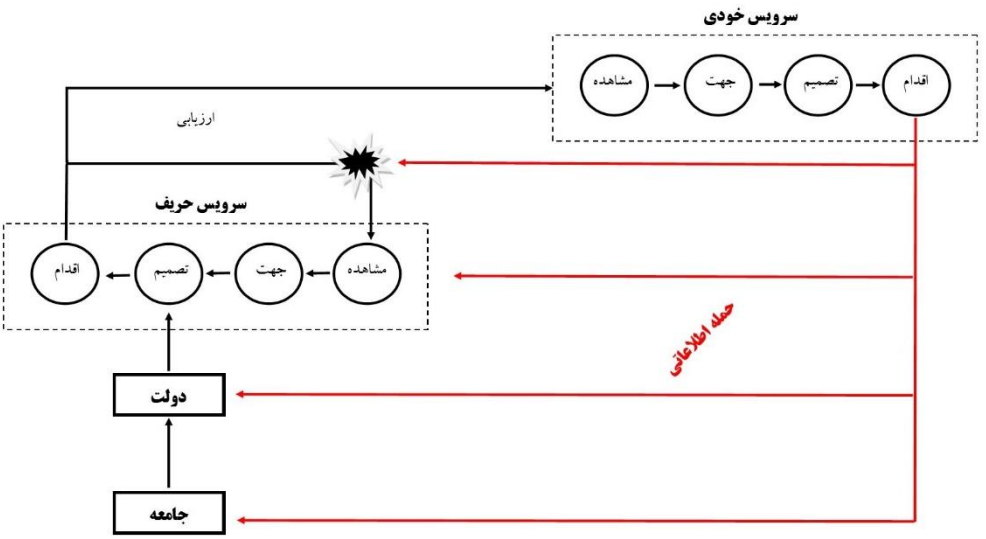
(والتز، ۳۴۷:۱۳۸۷). تقسیم‌بندی مهم‌تری که او از نوع اطلاعات تهاجمی ارائه می‌دهد، نوع هجوم است که فعال یا انفعالی باشد. نوع فعالانه که به آن نفوذ مستقیم گفته می‌شود، به هدف اطلاعاتی ـ برای مثال یک شبکه ارتباطاتی رایانه‌ای ـ نفوذ می‌کند تا بر محیط اطلاعات تسلط یافته یا دانش جدیدی کسب نماید؛ درحالی‌که حملات منفعلانه یا گیرنده‌های غیرمستقیم، به مثابه مشاهده‌گر بیرون سیستم اطلاعاتی رقیب یا دشمن، به رصد رفتارها، جریان اطلاعات، زمان‌بندی و دیگر مؤلفه‌های بیرونی ساختار حریف می‌پردازد (والتز، همان). ماتریس زیر، این تقسیم‌بندی را با درنظرگرفتن سه سطح فیزیکی، ساخت ارتباطی و ادراکی و هم‌چنین دو هدف کسب دانش یا اثرگذاری بر محیط اطلاعات نشان می‌دهد که مجموعاً برتری اطلاعاتی را هدف‌گذاری می‌کند.

جدول ۳. ماتریس سطوح تهاجم اطلاعاتی (والتز، ۳۵۳:۱۳۸۷)

هدف	کسب دانش		اثرگذاری بر محیط	
روش	مستقیم	غیرمستقیم	مستقیم	غیرمستقیم
سطح ادراکی	دسترسی به مذاکرات محرمانه به‌وسیله عامل انسانی	رصد رفتارها و مواضع و استنتاج فرآیندهای تصمیم‌گیری	ضداطلاعات و عملیات پنهان	فریب یا عملیات روانی به هدف مدیریت درک طرف مقابل
سطح زیرساختی	حمله شبکه‌ای و نفوذ برای تأمین دسترسی غیرمجاز	ره‌گیری ترافیک پیام‌ها به هدف تجزیه‌وتحلیل رمزگذاری	قطع سرویس با نفوذ ویروس درون شبکه اطلاعاتی	هدایت رفتار با ارسال پیام فریب یا انحراف ترافیک شبکه
سطح فیزیکی	سرقت تجهیزات	استراق سمع	فریب کاربر	حمله الکترونیکی

وقوع حملات مشکوک به تروریستی ۱۱ سپتامبر ۲۰۰۱، روند پژوهش‌های نظامی متمرکز بر تهاجم اطلاعاتی را دچار تحول مهمی کرد. اشغال پُرهزینه افغانستان و عراق ازسوی آمریکا، اعتراضات وسیعی در سطح توده‌ها، نخبگان اجتماعی و جنبش‌های مدنی ضدجنگ و به‌ویژه در مورد عراق را در برخی دولت‌های غربی برانگیخت؛ بنابراین کارشناسان نظامی و امنیتی به این نتیجه رسیدند که با وجود تجارب غرب در حوزه جنگ نرم، هم‌چنان نسبت به کسب سریع‌تر و کم‌هزینه‌تر اهداف مهم سیاسی، نظامی و امنیتی در قرن بیست‌ویک توانایی کافی ندارند. یکی از افرادی که با این دستورکار به مبحث تهاجم اطلاعاتی پرداخت، «بنیامین تونر» از فرماندهان ترکیه‌ای ناتو بود. او در پایان‌نامه

کارشناسی‌ارشد رشته مدیریت فناوری اطلاعات تحت عنوان «عملیات اطلاعاتی در سطوح تاکتیکی، عملیاتی و راهبردی جنگ: یک رویکرد متوازن سیستماتیک» ــ به راهنمایی دکتر «دنیل بوگر» مدیر گروه علوم رایانه دانشگاه تحصیلات تکمیلی نیروی دریایی آمریکا ـ به بررسی امکان‌مندی تلفیق سه سطح راهبردی، تاکتیکی و عملیاتی در جنگ اطلاعاتی پرداخته است. وی نبرد اطلاعاتی را نوعی از عملیات اطلاعاتی تعریف می‌کند که طی منازعه سخت به برتری اطلاعاتی بینجامد. برتری اطلاعاتی نیز حالتی است که به کیفیت، سرعت و کاهش هزینه تصمیم‌گیری نسبت به حریف منجر شود (Tuner, 2003, 5-6). او تهاجم اطلاعاتی را **کنترل محیط با هدف تأثیرگذاری بر فرآیند تصمیم‌گیری حریف** می‌داند که لازمه آن، درک صحیح و سپس تخریب یا اخلال در توان‌مندی‌های اطلاعاتی حریف است (Tuner, 2003, 12). وی مدل زیر را برای چگونگی تأثیرگذاری تهاجم ترسیم کرده است:



شکل ۷. فرآیند اثرگذاری تهاجم اطلاعاتی در مدل ترنر (Tuner, 2003:14).

در این مدل از چرخه مشاهده ـ جهت‌گیری ـ تصمیم ـ اقدام[1] موسوم به OODA برای توصیف عملکرد سازمان اطلاعاتی استفاده شده است. سرویس مهاجم پس از ارزیابی و پردازش داده‌های جمع‌آوری‌شده از وضعیت و توانایی‌های حریف، در چند مرحله اقدام به تهاجم اطلاعاتی می‌کند. ازآنجاکه حوزه نگارش این پایان‌نامه مبحث فناوری اطلاعات بوده،

1. Observe – Orient – Decide - Act

اتمسفر تهاجم در این مدل، بهره‌مندی از شبکه‌های اجتماعی و فضای سایبری برای متأثرساختن فضای ذهنی جامعه است که می‌تواند بر فضای نخبگان حاکم نیز تأثیرگذار باشد؛ ولی این کفایت نمی‌کند و می‌بایست فضای ادراکی دولت‌مردان حریف نیز، مستقیماً تحت حمله قرار بگیرد تا ضریب اطمینان تهاجم افزایش یابد. هم‌چنین با تأثیرگذاری بر وضعیت محیطی سرویس رقیب، در مرحله مشاهده و گردآوری داده‌های آن نیز اخلال ایجاد می‌شود. در پایان در مسیر ارزیابی، سرویس حریف در اقدام به مشاهده دوباره نیز اختلال ایجاد می‌کنند تا نتواند بازخورد مناسبی از اقدامی دریافت کند که آن نیز متأثر از مطلوبیت‌های خودی بوده؛ ولی خودش نسبت به ارزیابی تهاجم اقدام کرده و آن‌را به تجربه انباشته سرویس برای حملات بعدی می‌افزاید. ترنر و بوگر متأثر از تبعات تجاوز آمریکا به افغانستان و عراق، ثمرات یک عملیات اطلاعاتی تهاجمی را چنین برشمردند:

- افزایش قدرت آینده‌نگری نسبت به اهداف و مقاصد رقیب یا دشمن؛
- اثرگذاری بر رفتار دولت‌ها و سازمان‌های موافق و مخالف برمبنای روندی پایدار؛
- شکست مقاومت رهبران حریف؛
- تزلزل در اعتمادبه‌نفس نظامیان، دیپلمات‌ها و کارگزاران اقتصادی حریف؛
- اخلال در ارتباط‌گیری رهبران با مدیران و توده‌ها و
- تسخیر ذهن و قلب مردم جامعه هدف (Tuner, 2003:17).

نویسندگان، فریب نظامی، نبرد الکترونیک، جنگ سایبری و حملات بیولوژیک را ازجمله ظرفیت‌های عملیات اطلاعاتی دانسته‌اند که می‌بایست به‌وسیله ضدفریب، حمله نظامی و حفاظت‌های فیزیکی ـ اطلاعاتی پشتیبانی شوند و از توان‌مندی رسانه‌ها و جنبش‌های مدنی نیز برای تصویرسازی مطلوب از نیروی خودی و ترسیم چهره نامطلوب از دشمن بهره بگیرند (Tuner, 2003:34-38).

به‌مرور زمان و با گسترش ادبیات تهاجم اطلاعاتی، کاربرد آن در تقسیم‌بندی‌های آفندی و پدافندی نیز مورد توجه قرار گرفت. میشل کِلِیو، عضو مرکز ملی امنیت و ضداطلاعات در دولت بوش پسر، در مقاله «ضداطلاعات و امنیت ملی»، ازمنظر «ضداطلاعات تهاجمی» به مسأله نگریست. اهمیت این پژوهش از آن‌رو است که تهاجم، به‌مثابه رویکردی آفندی با حوزه ضداطلاعات، به‌عنوان اقدامی که عمدتاً دفاعی تلقی شده، چه نسبتی دارد. نویسنده، هدف ضداطلاعات تهاجمی را شکل‌دادن به چشم‌انداز و کاهش توان‌مندی‌های اطلاعاتی رقیب خارجی (Cleave, 2007:3) و شیوه آن‌را استفاده از عملیات اطلاعاتی رقیب علیه خودش، عنوان نمود (Cleave, 2007:9). به‌طور مثال، می‌توان

داده‌های محیطی را به‌نحوی دست‌کاری کرد کـه عملیـاتِ جمـع‌آوریِ منـتج بـه محصـول اطلاعاتی رقیب، تصمیم‌گیری او را به‌سوی منافع خودی متأثر سـازد (Cleave, 2007, 10). به بیان دیگر، ضداطلاعات تهاجمی، تسلط بر ادراک حریف از **ما** بـه‌واسـطه دخالـت مـا در عملیات اطلاعاتی اوست؛ چنان‌چه دیگر پژوهش‌ها نیز ضداطلاعات تهاجمی را وارونه‌سـازی اهداف دشمن با آشفته‌سازی ذهنی او تعریف کرده‌اند، به‌طوری‌که بـا هـدایت او بـه فضـای نادرست، فریب بخورد (علی‌خانی، ۳۴۷:۱۳۹۴). علاوه‌براین، در سندی بی‌تاریخ از کتابخانـه سیا که با توجه به محتوای آن، مربوط به جنگ سرد طی ۱۹۵۰ تا ۱۹۷۰ است نیز، هـدف عملیات تهاجمی در ضداطلاعات، تخریب، غافلگیری و بـی‌اعتبارسـازی سـرویس اطلاعـاتی رقیب عنوان شده است (No named, No Date, 2). جدول زیر، مرور ادبیات لاتین اطلاعات تهاجمی را ترسیم می‌کند:

جدول ۳. مرور ادبیات لاتین تهاجم اطلاعاتی.

سال	نویسنده	مفهوم
۱۹۹۶	جرج استین	اختلال در فرآیند شناختی طرف مقابل
۱۹۹۹	مارتین لیبیسکی	ضربه مخفی به نخبگان طرف مقابل
۱۹۹۹	پائول ژاویدنیاک	حمله‌ای به درون سیستم حریف
۱۹۹۹	دوروتی دنینگ	کاهش محرمانگی، جامعیت و دسترس‌پذیری اطلاعات حریف
۱۹۹۹	دونالد ولز	سلب ابتکار عمل حریف
۱۹۹۹	الکساندر وودکوک	نفوذ بر تصمیم‌گیران طرف مقابل
۲۰۰۰	اِد والتز	پذیرش مطلوبیت مهاجم به‌مثابه منافع خودی
۲۰۰۳	بنیامین تونر	کنترل محیط تصمیم‌گیری حریف
۲۰۰۷	میشل کِلِیو	تسلط بر ادراک حریف

جمع‌بندی ادبیات مشاهده‌شده در حوزه تهاجم اطلاعـاتی را مـی‌تـوان در تعبیـر دکتـر «استفان گابریل» کارشناس اطلاعـاتی وزارت دفـاع و اسـتاد دانشـگاه دفـاع ملـی رومـانی مشاهده کرد که «رویکرد تهاجمی در حوزه‌های اقتصادی، فرهنگی، سایبری و اطلاعاتی در انواع جنگ‌های جدید، با هدف **غلبه‌بر ذهن و تغییرنگـرش تصـمیم‌گیـری** طـرف مقابـل صورت می‌پذیرد» (Gabriel, 2016:7)؛ زیرا تغییر ذهنیت دولـت‌مـردان و سیاسـت‌گـذاران مطابق میل نیروی مهاجم، منافعی به‌مراتب بلندمدت‌تر از پیروزی‌های میدانی دارد.

نتیجه‌گیری

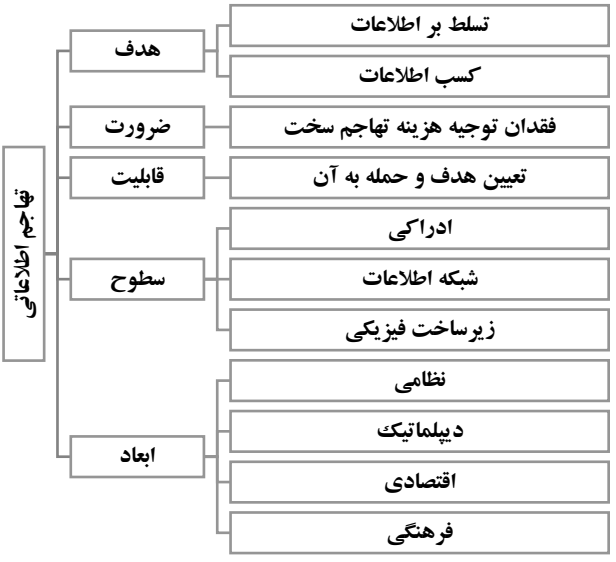
اطلاعاتِ تهاجمی در عرصه امنیتی، بدواً معطوف به اثرگذاری بر قوه تحلیل جامعه هدف به‌ویژه نخبگان اجتماعی تعریف شده بود؛ به‌گونه‌ای که می‌توان آن‌را مترادف جنگ نرم یا در ابعاد فنی‌تر، عملیات روانی قلمداد کرد. با این حال، به‌تدریج ورود سرویس‌های اطلاعاتی به این حوزه، هم مخاطب را ازمنظر سطح اقتدار و هم روش را، ازنظر دقت هدف‌گذاری ارتقا داد، به‌نحوی‌که تهاجم اطلاعاتی منجر به سلب ابتکار عمل مقامات تصمیم‌ساز در ساختار دولت یا گروه‌های فراملی/فروملی حریف شده و با اخلال در فرآیند شناختی و ادراکی، وی را تحت تسلط اراده خودی گرفتار نماید. این مسأله به‌خصوص در شرایطی که تهاجم علنی در حوزه‌های نظامی، امنیتی، سیاسی، دیپلماتیک و اقتصادی پُرهزینه و خطرناک‌تر باشد، اهمیت اساسی دارد. ضرورت رویکرد تهاجمی به اطلاعات را زمانی می‌توان دریافت که به‌واسطه آینده‌پژوهی، سناریوهای توطئه‌چینی محتمل مدنظر قراربگیرد و برای گریز از یک پاسخ پُرهزینه در آینده نزدیک، طراحی آتی دشمن را به‌نفع نیروی خودی تغییر دهد. به بیان دیگر، زمین بازی طرف دیگر، بدون آنکه خود دریابد، توسط ما تدوین شود و او به‌خیال آنکه درصدد عملیات علیه ماست، در پازلی گام بردارد که پیش‌تر سناریوهایش در اتاق فکر خودی طرح شده است. نتیجه رویکرد تهاجمی به اطلاعات، هم تسلط بر محیط اطلاعاتی حریف اعم از کسب و تحلیل اطلاعات از سوی اوست و هم می‌تواند افزایش اطلاعات مهاجم باشد. نکته دیگر اینکه آماج تهاجم، صرفاً دشمن یا حتی رقیب نیست بلکه می‌تواند مؤتلف یا حتی متحد طرف مهاجم باشد؛ زیرا گاهی اوقات ـ و ازقضا شاید درباره بازیگران متحد، بیش از بازیگران رقیب و متخاصم ــ لازم است که از رویکرد تهاجمی به اطلاعات بهره گرفته شود؛ زیرا اگر در مواردی درباره دشمن، امکان تهاجم نظامی، امنیتی و سیاسی دشوار باشد، درباره دوست ممکن است حتی به‌فرض امکان‌مندی، بی‌فایده و خلاف مصلحت باشد. این مسأله می‌تواند حتی در پوشش یک مشورت دوستانه و در ظاهری کاملاً غیرتهاجمی رخ بدهد. به‌واقع اطلاعات تهاجمی، برخلاف عنوانش صرفاً در فضایی تقابل‌جویانه رخ نمی‌دهد؛ بلکه به جهت ماهیت نرم‌افزاری و مبتنی بر دستاویز داده‌های محیطی، مهاجم می‌تواند در چهره‌ای غیرخصمانه ظاهر شود.

با توجه به ابعاد گوناگون تهاجم اطلاعاتی از نظامی و سیاسی تا اقتصادی و فرهنگی، ابزارهای اجرای آن از قدرت سخت مانند حمله فیزیکی به ساختارهای شناسایی حریف به هدف اخلال در مخابره پیام از محیط؛ قدرت نیمه‌سخت مانند تحریم‌های اقتصادی برای تغییر محاسبات او یا قدرت نرم چون عملیات روانی و دیپلماسی عمومی را دربرمی‌گیرد.

به‌همین‌ترتیب، مجریان این دسته اقدام‌ها نیز از سازمان‌های نظامی، سرویس‌های اطلاعاتی، وزارت خارجه، وزارت اقتصاد، بانک مرکزی تا شبکه‌های تلویزیونی، مطبوعات و نهادهای مردمی، متفاوت هستند. بالاترین سطح اطلاعات تهاجمی تغییر ادراک سوژه است؛ ولی سطوح پایین‌تر می‌تواند هدف‌گیری شبکه اطلاعاتی حریف مانند شبکه‌های اجتماعی و کانال‌های تبادل اطلاعات یا در سطحی کمتر، زیرساخت فیزیکی مانند اماکن و تجهیزات مورداستفاده‌اش در چرخه اطلاعات باشد. هر یک از این سه سطح بسته به موقعیت، موضوع و زمان‌بندی، می‌تواند دستاوردی راهبردی، عملیاتی یا تاکتیکی محسوب شود. با توجه به موارد مذکور می‌توان تهاجم اطلاعاتی را چنین تعریف کرد:

«نوعی حمله پیش‌دستانه به چرخه اطلاعاتی، منتج به تصمیم‌سازی دولت/سازمان‌های متحد، مؤتلف، رقیب یا متخاصم که به هدف مدیریت ادراک و تغییر محاسبات آن، زمین بازی را مطابق منافع خودی طراحی می‌کند و به مهار یا تغییر رفتار طرف مقابل بینجامد.»

ازآنجاکه تولید ادبیات تهاجم اطلاعاتی در ابتدای راه قرار دارد، نمی‌توان مدعی شد این تعریف کاملاً جامع و مانع است؛ ولی به‌نظر می‌رسد بتوان این ادعا را مطرح نمود که می‌تواند آغاز مناسبی برای دیگر پژوهشگرانی باشد که بتوانند به تکمیل آن اقدام نمایند. به‌همین‌دلیل می‌توان مؤلفه‌های تهاجم اطلاعاتی را برمبنای تعریف مذکور، به شکل زیر ترسیم کرد:



شکل ۸ عناصر تهاجم اطلاعاتی

بدون شک توجه پژوهشگران حوزه امنیت ملی ازجمله در مباحث سیاست خارجی و مطالعات اطلاعاتی، می‌تواند به تکمیل ادبیات تهاجم اطلاعاتی کمک کرده و علاوه‌بر حوزه نظری، ازمنظر اجرایی نیز دستگاه‌های تصمیم‌ساز و تصمیم‌گیر در نظام جمهوری اسلامی را در زمینه مقابله با تهاجم اطلاعاتی دشمن، ایده‌پردازی و در طراحی عملیات‌های تهاجمی، یاری رساند.

منابع

فارسی

دنینگ، دورتی (۱۳۸۳)، *جنگ اطلاعات و امنیت*، گروه مترجمان، پژوهشکده پردازش هوشمند علائم، تهران.

رشیدزاده، فتح‌الله (۱۳۸۵)، *عصر اطلاعات و جنگ اطلاعاتی*، فصل‌نامه مدیریت نظامی، شماره ۲۱.

صابرفرد، علیرضا (۱۳۹۱)، *تحلیل سناریویی، رویکردی نوین در تحلیل و آینده‌نگاری اطلاعاتی ـ امنیتی جامعه اطلاعاتی*، فصل‌نامه پژوهش‌های حفاظتی و امنیتی، شماره ٤.

فضائلی، علی (۱۳۷۸)، *نبرد اطلاعاتی: جنگ در عصر اطلاعات*، فصل‌نامه اطلاع‌شناسی، شماره ۱۹.

علی‌خانی، علی (۱۳۹٤)، *آرا و نظریه‌ها در اطلاعات*، انتشارات دانشکده اطلاعات و امنیت ملی، تهران.

معاونت پژوهش و تولید علم (۱۳۹۵)، *نظریه و روش در اطلاعات*، انتشارات دانشکده اطلاعات و امنیت ملی، تهران.

والتز، ادوارد (۱۳۸۷)، *عملیات و اصول جنگ اطلاعات*، ترجمه غلامعلی جانگذار، معاونت پژوهشی دانشکده امام باقر(علیه‌السلام)، تهران.

انگلیسی

Bishop. Matt, (2003), *the Strategy and Tactics of Information Warfare*, Contemp Security Policy, Volume 24, Number 1

Chairman of the Joint Chiefs of Staff, (2013), *Joint Intelligence*.

Cleave. Michelle, (2007), *Counterintelligence and National Strategy*, School for National Security Executive Education of National Defense University.

Gabriel. Stefan, (2016), *a contemporary military phenomenon in the light of critical* infrastructure, the 11th International scientific conference "defense resources management", Romania.

Hirschland. Matthew, (*2001), Information Warfare and the New Challenges to Waging Just War, American Political Science Association's Annual Meeting.*

Libicki. Martin, (1999), *The Changing Role of Information in Warfare*, "Strategic Appraisal: The Changing Role of Information in Warfare", Publisher: Rand Corporation.

No named, (No date), *conduct offensive (strategic) counterintelligence operations in furtherance of national security policy initiative*, CIA-Doc:0000112364.

Stein. Georg, (1996), *Information Attack, Information Warfare in 2025*, Air War College.

Tuner. Bunyamin, (2003), *Information Operations in Strategic, Operational, and Tactical Levels of War: A Balanced Systematic Approach*, Master's Thesis, Naval Postgraduate School.

Welch. Donald, (1999), *Strike Back: Offensive Actions in Information Warfare*, United States Military Academy.

Woodcock. Alexander, (1999), *Information Operations in Support of Civil-Military*

Interactions, Conference Analysis of Civil-Military Interactions.
Waltz. Edward, (2000), *Data Fusion in Offensive and Defensive Information Operations*, National symposium of sensor and data fusion.
Zavidniak. Paul, (1999), *Achieving Information Resiliency*, Information Technology Security Report, Volume 4, Number 3.

Conceptualization of Offensive Approach to Intelligence

Ehsan Kiani [1]
Hadi Tajik [2]

While the importance of intelligence battles in international conflicts is not obscured, achieving a relatively accurate definition of offensive approach to intelligence can help national security decisionmakers both defensively to identify intelligence's attacks and design offensive strategies. In order to produce Persian-language literature on offensive intelligence, this study based on the evaluation of explicit Latin research with a descriptive-analytical method from library collection, attempts to explain the issue of offensive intelligence. Assessing the definitions of this approach in Western sources shows that offensive intelligence can be considered as a preemptive attack on the intelligence cycle resulting in the decision of the rival government or groups to design the playground according to its own interests. And leads to control or change the behavior of the rival. In an offensive approach to intelligence to change the balance of power, it is necessary to capture the pulse of the opponent's functional data in order to influence the enemy's plans and even direct them according to their own interests.

Keywords
Offensive Intelligence, Intelligence Superiority, Field Awareness, Dominant Knowledge

1. PH.D Candidate, Imam Hossein University, Tehran, Iran
E1386k@gmail.com
2. Assistant Professor, Imam Hossein University, Tehran, Iran
Int.1358@yahoo.com