
بسم الله الرحمن الرحيم

توان سایبری ناتو:
تکامل استراتژیک و عملیاتی

گزیده پژوهش‌های جهان: توان سایبری ناتو: تکامل استراتژیک و عملیاتی
بررسی و نظارت: مؤسسه فرهنگی مطالعات و تحقیقات بین‌المللی ابرار معاصر تهران ـ معاونت پژوهشی
ترجمه و تلخیص: حسین عسگریان
تاریخ انتشار: ۹۶/۵/۷
تلفن و دورنگار: ۷ ـ ۸۸۷۵۶۲۰۵
صندوق پستی: ۳۸۴۹ ـ ۱۵۸۷۵
نشانی اینترنت: www.tisri.org

توان سایبری ناتو:
تکامل استراتژیک و عملیاتی[1]

توسعه توان دفاع سایبری سازمان پیمان آتلانتیک شمالی (ناتو) از زمان کنفرانس پراگ در سال ۲۰۰۲ پیشرفت مستمری را داشته است. با توجه به حملات سایبری فراوان ازجمله حمله به استونی در سال ۲۰۰۷، اولویت‌های این اتحادیه در زمینه سیاست‌های دفاع سایبری تکامل یافته و در سال‌های ۲۰۰۸، ۲۰۱۱ و ۲۰۱۵ مورد بازنگری قرار گرفته است. متن حاضر به بررسی وضعیت گذشته و تکامل تلاش‌های دفاع سایبری ناتو ازطریق ارزیابی کارآمدی این سیاست‌ها در پیش‌بینی تهدیدات علیه کشورهای عضو، ازجمله ایالات متحده آمریکا پرداخته است. براین‌اساس، این گزارش بر تاریخ تلاش‌های دفاع سایبری ناتو و اینکه چگونه استراتژی و سیاست‌های این اتحادیه با توجه به شرایط تغییر نموده، متمرکز شده است.

نویسنده در سه بخش به تبیین استراتژی و سیاست دفاع سایبری ناتو، توان سایبری این اتحادیه و مأموریت‌های آن و درنهایت، مسائل و چالش‌های اصلی پیشِ روی سیاست کنونی ناتو پرداخته است. براین‌اساس، در بخش اول توان فضای سایبری ناتو و استراتژی و سیاست این اتحادیه را در این حوزه بررسی نموده است. در این بخش نویسنده، تکامل بنیان‌های استراتژیک فعالیت‌ها، سیاست‌ها و چگونگی هدایت سایبری ناتو و تکامل آنها در طی سیزده سال گذشته را شرح داده و درهمین‌راستا، به تحلیل مسائل مطرح در نشست‌های سران در ارتباط با دفاع سایبری و سیاست‌های دفاع سایبری رسمی ناتو از سال ۲۰۰۲ به بعد متمرکز شده است.

در بخش دوم، به توان فضای سایبری ناتو با تمرکز بر حوزه نظامی و نیز موارد زیر توجه

1. Jeffery L. Caton, "NATO Cyberspace Capability: A Strategic and Operational Evolution, Strategic Studies Institute, Aug 2019, 111pp.

گردیده است: وظایف و مأموریت‌های دفاع سایبری ناتو در حوزه‌هایی مثل: حفاظت از شبکه ناتو، آگاهی وضعیتی مشترک در فضای سایبر، حفاظت از زیرساخت‌های حیاتی، مبارزه با تروریسم، پشتیبانی از توسعه توان سایبری کشورهای عضو، و واکنش به بحران‌های مربوط به فضای سایبری. نویسنده در این بخش ازطریق بررسی عملیات‌ها و برنامه‌ریزی، دکترین‌ها و روش‌ها، آموزش و مانورهای مربوط به فعالیت‌های سایبری نظامی ناتو، به تشریح توان سایبری ناتو در این حوزه‌ها پرداخته است؛ اما در بخش سوم، مهم‌ترین مسائل مربوط به سیاست کنونی دفاع سایبری ناتو در مرکز توجه قرار گرفته است. براین‌اساس، مسائل مربوط به فضای سایبری تهاجمی، بازدارندگی ازطریق فضای سایبر، الزامات قانونی و همکاری با اتحادیه اروپا بررسی شده است. برخی از مهم‌ترین نکات مطرح در این گزارش به‌قرار زیرند:

ـ اصول بنیادین ناتو شامل دفاع جمعی، مدیریت بحران و امنیت همیارانه در میان کشورهای عضو است. بعد از تغییرات در نظام جهانی، سقوط پیمان ورشو، سپری شدن دوره‌ای چندین‌ساله، این اتحادیه رنسانسی را در کارکرد اصلی امنیتی خود تجربه کرد و مفهوم جدید استراتژیک در سال ۲۰۱۰ مورد پذیرش قرار گرفت.

ـ در کنفرانس سران شورای آتلانتیک شمالی (NAC) در پراگ جمهوری چک در سال ۲۰۰۲، دفاع سایبری به‌عنوان موضوع مهم و ارزشمندی در این اتحادیه مطرح شد. سران ناتو در این نشست ایجاد یک برنامه دفاع سایبری فنی شامل تأسیس توان واکنش به وقایع کامپیوتری ناتو (NCIRC) را تصویب نمودند. در آن زمان، کار در حوزه دفاع سایبری درحال پیشرفت بود، اما تا زمان برگزاری کنفرانس سران ریگا در لیتوانی در سال ۲۰۰۶، هیچ اشاره‌ای در کنفرانس‌های سران ناتو به این موضوع صورت نگرفت. در این نشست، کار برای توسعهٔ شبکه‌ای به‌منظور تبادل اطلاعات در عملیات‌های ناتو و بهبود و ارتقاء حفاظت در برابر حملات سایبر مورد پذیرش قرار گرفت.

در ادامه، در نشست سران ۲۰۰۸ بوداپست مجارستان، ابتکار سیاسی در زمینه دفاع سایبری و توسعه ساختارها و اختیارات برای اجرای آن تصویب شد. در کنفرانس سران ۲۰۰۹ در استراسبورگ و کلن در فرانسه و آلمان، ایجاد اداره مدیریت دفاع سایبری ناتو (CDMA)، ارتقاء توان واکنش به وقایع کامپیوتری و فعال شدن مرکز عالی دفاع سایبری مشترک (CCD COE) در استونی مورد پذیرش قرار گرفت. در کنفرانس سران لیسبون پرتغال در سال ۲۰۱۰، اعضا خواهان بازنگری در سیاست دفاع سایبری ناتو تا ژوئن ۲۰۱۱ و پشتیبانی از برنامه عمل

این اتحادیه شدند. علاوه‌براین، در این نشست، اعضا خواستار تسریع در رسیدن به توان کامل عملیاتی، توان واکنش به وقایع کامپیوتری، و قرار گرفتن همه اجزاء ناتو تحت حمایت سایبری متمرکز شدند. همکاری نزدیک با دیگر بازیگران مثل: سازمان ملل متحد و اتحادیه اروپا از دیگر تصمیمات در نشست سران لیسبون محسوب می‌گردد. در کنفرانس سران ایلینویز در سال ۲۰۱۲ در آمریکا، مفهوم سیاست و برنامه عمل سایبری جدید پذیرفته شد و در کنفرانس نیوپورت ولز در سال ۲۰۱۴، سیاست دفاع سایبری ارتقایافتهٔ ناتو مورد تصویب قرار گرفت.

ـ نتیجه مهم کنفرانس سران لیسبون در سال ۲۰۱۰، پذیرش مفهوم استراتژیک جدید ناتو: تعامل فعال و دفاع مدرن بود. این سند رسمی اهداف پایدار، وظایف امنیتی اساسی و محیط امنیتی قابل پیش‌بینی ناتو را توصیف نموده و نیز راهنمایی برای نیروهای نظامی بوده است که بدانند چگونه باید اجزای این مفهوم جدی را بپذیرند. تعامل فعال و دفاع مدرن بر سه وظیفه اصلی متمرکز است: دفاع جمعی، مدیریت بحران، و امنیت همیارانه. در بخش محیط امنیتی این سند به فراگیر شدن، سازمان‌یافته شدن و هزینه‌ساز شدن حملات سایبری علیه دولت‌ها و صنایع اشاره شده و آمده است که چنین حملاتی ممکن است نه‌تنها ازسوی نیروهای نظامی خارجی، بلکه ازسوی مجرمان سازمان‌یافته، تروریست‌ها و گروه‌های افراط‌گرا صورت گیرد. علاوه‌براین، این سند به حوزه گسترده‌ای از توانمندی‌های مورد نیاز برای مقابله با حملات سایبری پرداخته است.

ـ سیاست دفاع سایبری ناتو در کنفرانس سران بخارست در سال ۲۰۰۸ تصویب شد. این سیاست در سال ۲۰۱۱ بعد از کنفرانس سران لیسبون به‌روز شد و بار دیگر در کنفرانس سران در ولز در سال ۲۰۱۴ مورد بازنگری قرار گرفت. اصول اصلی این سیاست در طی این سه نشست براساس موارد زیر بوده است: در کنفرانس سران ۲۰۰۸ بخارست بر حفاظت از نظام‌های اطلاعاتی کلیدی، بهترین رویه‌های مشترک برای دفاع سایبری، توسعه توان برای کمک به کشورهای متحد برای مقابله با حملات تروریستی و تقویت پیوند میان ناتو با مقامات ملی تأکید شده بود. در سال ۲۰۱۱ بر پیشگیری، انعطاف و دفاع از دارایی‌های سایبری حیاتی ناتو و متحدان این اتحادیه، توسعه توان دفاع سایبری و حفاظت متمرکز از شبکه‌های متعلق به ناتو، توسعه حداقل‌های نیاز دفاع سایبری شبکه‌های ملی، تدارک کمک به متحدان برای دستیابی به حداقل سطح دفاع سایبری و کاهش آسیب‌پذیری‌های زیرساخت‌های حیاتی ملی، تعامل با شرکا، سازمان‌های ملی، بخش خصوصی و مراکز آکادمیک تأکید شده بود. در سال

۲۰۱۴، بر اصول جدایی‌نشدنی امنیت متحدان و پیشگیری، کشف، انعطاف، احیاء و دفاع تأکید دوباره شد و سران در این نشست خواستار مسئولیت دفاع سایبری بنیادین ناتو در دفاع از شبکه‌های این اتحادیه شدند. علاوه‌براین، تأکید بر مسئولیت متحدان برای توسعه توان مربوط به حفاظت از شبکه‌های ملی خود، شناسایی کاربردپذیری حقوق بین‌الملل در فضای سایبری، تأکید دوباره بر دفاع سایبری به‌عنوان وظیفه اصلی ناتو براساس ماده پنج مربوط به دفاع جمعی در این نشست مورد اشاره قرار گرفت.

ـ سیاست دفاع سایبری ارتقایافتهٔ ناتو در سال ۲۰۱۴ بر بهبود فرایندهای حکمرانی سایبری تأکید می‌کند و رسماً حوزه سایبری را به وظیفه سنتی اصلی ناتو یعنی دفاع جمعی پیوند می‌دهد. بااین‌حال، تأکید دارد که دفاع سایبری ناتو در درجه اول برای دفاع از شبکه‌های خود بوده و لذا کشورهای عضو به‌طور جداگانه باید دفاع از شبکه‌های ملی‌شان را مورد توجه قرار دهند. این سیاست همچنین رسماً اعلام می‌نماید که حقوق بین‌الملل در فضای سایبری کاربردپذیر است. دراین‌میان، مسئولیت دفاع و مدیریت دفاع سایبری برعهده شورای آتلانتیک شمالی است و کمیته دفاع سایبری تحت نظارت آن اقدام می‌کند.

ـ ناتو در راستای سیاست دفاع سایبری کنونی خود اولویت اصلی را به حفاظت از نظام‌های ارتباطاتی و اطلاعاتی خود داده است. این نظام‌ها از عملیات‌های نظامی این سازمان پشتیبانی می‌کنند. ناتو همچنین چندین مأموریت پشتیبانی و حمایتی مهم ازجمله آگاهی وضعیتی مشترک در فضای سایبر، حفاظت از زیرساخت‌های حیاتی، حفاظت از زیرساخت‌های اطلاعاتی حیاتی، مبارزه با تروریسم، حمایت از توسعه توان سایبری کشورهای عضو و واکنش به بحران‌های مرتبط با فضای سایبری را مورد تأکید قرار داده است. برای تشریح وظایف این حوزه، بررسی عملیات‌ها و برنامه‌ریزی، دکترین و روش‌ها، آموزش و تمرین‌های مربوط به فعالیت‌های فضای سایبری نظامی ضروری است.

ـ همان‌گونه که شورای آتلانتیک شمالی، سیاست و مسیر استراتژیک را تعیین می‌کند، کمیته‌های ستاد ناتو چگونگی اداره و فرماندهی عملیات‌های متحد، و برنامه‌ریزی و اجرای همه عملیات‌های این اتحادیه را برعهده دارند. فرماندهی عملیات‌های متحد، برای دستیابی به وظیفه اصلی تضمین تمامیت ارضی این اتحادیه و پشتیبانی از مأموریت‌های این سازمان که ممکن است مستلزم استقرار نیروها در خارج باشد، در سطوح استراتژیک، عملیاتی و تاکتیکی عمل می‌نماید. عملیات‌هایی در سطح استراتژیک در ستاد عالی قدرت‌های اروپایی متحد، که

در بلژیک مستقر است هدایت می‌گردد. مأموریت‌ها در سطوح عملیاتی متکی بر فرماندهی نیروهای مشترک در هلند، و در ناپل ایتالیا هستند. عملیات‌ها در سطوح تاکتیکی ازسوی سه فرماندهی اصلی شامل: ستاد فرماندهی نیروهای زمینی متحد، در ازمیر ترکیه، ستاد فرماندهی نیروی دریایی متحد، در نیوتاون انگلستان و ستاد فرماندهی هوایی متحد، در رامشتاین آلمان هدایت می‌گردد. سازمان عملیات‌های سایبری ناتو از پارادایم مشابه پیروی می‌نماید. دفاع سایبری در سطوح استراتژیک و آگاهی وضعیتی در فرماندهی عملیات‌های ائتلاف، فعالیت‌های سایبری در سطوح عملیاتی در فرماندهی‌های نیروهای مشترک، در فرماندهی‌های تاکتیکی و در گروه نظام‌های ارتباطاتی و اطلاعاتی، هدایت می‌گردد. آگاهی وضعیتی سایبری در سطح تاکتیکی در درجه اول ازسوی آژانس ارتباطات و اطلاعات ناتو اداره می‌گردد. این آژانس از عملیات‌های روزانه فرماندهی عملیات‌های متحد حمایت می‌کند و وظیفه اصلی آن، ارتباط و دفاع از شبکه‌های متحدان و همچنین کمک به ناتو و کشورهای متحد این سازمان در توسعه توان اطلاعاتی و ارتباطی است.

ـ فرماندهی دگرگونی متحد، یکی از دو فرماندهی استراتژیک ناتوست که به‌همراه فرماندهی عملیات‌های متحد، به ساختار فرماندهی ناتو شکل می‌دهد. درحالی‌که فرماندهی عملیات‌های متحد، بر عملیات‌های کنونی متمرکز است، فرماندهی دگرگونی متحد، تمرکز خود را بر ابتکارات تغییردهنده برای ساختار نظامی ناتو، نیروها، توانمندی و دکترین این اتحادیه گذاشته است. ستاد اصلی این فرماندهی در نورفولک ویرجینیا قرار دارد و سه واحد اصلی آن عبارتند از: مرکز جنگ مشترک در استاوانگر نروژ؛ مرکز آموزش نیروهای مشترک در بید گوشچ لهستان؛ و مرکز تحلیل و فراگیری در مونسانتو پرتغال. دیگر مراکز آموزشی و تحصیلی و مراکز عالی فعالیت‌های خود را با فرماندهی دگرگونی متحد هماهنگ می‌نمایند. وضعیت توسعه دکترین عملیات‌های فضای سایبر هنوز در مرحله شکل‌گیری است. نگاهی به اسناد در دسترس مرتبط با دکترین مشترک متحد ناتو نشان‌دهنده عدم یکپارچگی در فعالیت‌های سایبری ناتوست.

ـ موضوع آموزش و تمرین در حوزه فضای سایبری در سطوح چندگانه در ناتو پیگیری می‌گردد. کالج دفاعی ناتو در رم ایتالیا مسائل مربوط به دفاع سایبری در سطح استراتژیک را با تمرکز بر پیامدهای گسترده‌تر ژئوپلیتیک آن پوشش می‌دهد. مدرسه ناتو در آلمان اخیراً شش رشته درسی مرتبط با عملیات‌های اطلاعاتی و سایبری را در سطوح عملیاتی و در راستای

حمایت از افسران ستاد و پرسنل امنیت سایبری ناتو ایجاد نموده است. مرکز جنگ مشترک ناتو آموزش برای ستادها در سطوح عملیاتی و مشترک را درنظر گرفته است. علاوه‌براینها، در چندین مرکز آموزشی ناتو موضوع آموزش فضای سایبری مورد تأکید قرار گرفته است.

بزرگ‌ترین مانور و تمرین دفاع سایبری ناتو با عنوان «ائتلاف سایبری» از سال ۲۰۰۸ هر ساله برگزار شده است. در مانور ائتلاف سایبری سال ۲۰۱۴ بیش از ششصد نفر از متخصصان سایبری از بیش از دوازده کشور عضو ناتو یا متحد این سازمان شرکت نمودند. این متخصصان هم در حوزهٔ دانشگاه و هم در حوزهٔ صنعت فعالیت می‌کردند. این مانور همچنین به‌عنوان یک آزمایش برای نظام اطلاعاتی سایبری و هماهنگی وقایع، تحت ابتکار دفاع هوشمند ناتو عمل می‌کند. ائتلاف سایبری ۲۰۱۴ به‌عنوان صحنه‌ای برای تبادل اطلاعات در سطوح استراتژیک و عملیاتی، تصمیم‌گیری در سطوح ارشد، هماهنگی چندسطحی در حوزه سایبر در میان ۲۶ عضو ناتو و پنج کشور شریک مشارکت‌کننده در این مانور عمل نموده است.

ـ موضوع استفاده از سایبر تهاجمی ازسوی ناتو یکی از مشکلات عملیات‌های فضای سایبری برای این اتحادیه است. دراین‌میان، موضوع اصلی برای دکترین سایبری ناتو این است که چرا فاقد توان سایبری تهاجمی تأثیرگذار بر پیشگیری یا دفاع سایبری است. به‌طور کلی، عملیات‌های سایبری تهاجمی ممکن است به‌عنوان استفاده از توان سایبری خارج از حوزه دفاعی شبکه ناتو موردنظر قرار گیرد. پیامد چنین استفاده‌ای علیه یک کشور خارجی تصور استفاده از سلاح هسته‌ای را در ذهن می‌آورد. درواقع، برخی کارشناسان تأکید می‌کنند که در داخل ناتو یک باشگاه سایبری وجود دارد (آمریکا، انگلستان، و فرانسه) که نه‌تنها دارای سلاح هسته‌ای هستند، بلکه توان فضای سایبری تهاجمی فعال را نیز دارند. به‌طور کلی، ممکن است ناتو درحال ورود به منطقه خاکستری توسعه توان دفاع سایبری فعال فراتر از ایجاد دیوار آتش برای خنثی‌سازی حملات اینترنتی خاص همانند آنچه استونی در سال ۲۰۰۷ تجربه نمود، باشد. دراین‌میان، باید اشاره نمود که مفهوم عملیات سایبری تهاجمی می‌تواند به‌عنوان بخشی از توانمندی تلقی شود که نقشی در بازدارندگی دارد.

ـ ایالت متحده آمریکا تنها کشوری است که به‌طور رسمی بازدارندگی را به‌عنوان بخشی از استراتژی بین‌المللی خود اعلام نموده است. ازآنجاکه حمایت از متحدان به صراحت در سیاست‌های آمریکا مورد تأکید قرار گرفته است، ناتو نیز تحت چتر حمایت بازدارندگی سایبری آمریکا قرار دارد.

ـ یکی از مسائل مورد توجه و مناقشه‌برانگیز هم در ناتو و هم در جامعه جهانی، موضوع چگونگی کاربردپذیری حقوق بین‌الملل در فعالیت‌های فضای سایبری است. از چشم‌انداز امنیتی، پیشرفت قابل‌توجهی دراین‌زمینه با انتشار دستورالعمل تالیان صورت گرفته است. این دستورالعمل توسط گروهی از متخصصان بین‌المللی که توسط مرکز عالی دفاع سایبری ناتو دعوت شده بودند، طی سه سال تدوین شده است. این دستورالعمل دربارهٔ کاربرد حقوق بین‌الملل بر جنگ سایبری است که در سال ۲۰۱۳ منتشر شده و عمدتاً متمرکز بر جنگ سایبری علیه بازیگران کشوری در سطحی است که حملات مسلحانه را دربرگیرد.

ـ اعلامیه کنفرانس سران ناتو در لیسبون خواستار همکاری نزدیک ناتو با اتحادیه اروپا در حوزه دفاع سایبری شده بود. درواقع، از ۲۸ عضو ناتو همگی به‌جز آلبانی، کانادا، ایسلند، نروژ، ترکیه و آمریکا جزو اتحادیه اروپا محسوب می‌گردند. این کشورها دارای منافع مشترک در برنامه‌های امنیتی هدایت‌شده ازسوی هر دو سازمان هستند. در حوزه امنیت سایبری، هر دو گروه دارای اهداف مشترک، اما رهیافت‌های متفاوتند. به گفته برخی کارشناسان، برای ناتو و اتحادیه اروپا امنیت سایبری یک موضوع استراتژیک است که بر امنیت دفاع کشورهای عضو و خود این دو سازمان تأثیرگذار است. دراین‌میان، وظایف هر دو سازمان می‌تواند مکمل هم باشد. ناتو به‌طور خاص بر جنبه‌های امنیتی و دفاعی امنیت سایبری متمرکز است و اتحادیه اروپا به موضوع گسترده‌تری یعنی طیف غیرنظامی مسائل سایبری (مثل: آزادی و حکمرانی اینترنت، حقوق آنلاین، حفاظت از داده‌ها) و جنبه‌های امنیت داخلی می‌پردازد.

ـ برخی مطالعات از بهبود همکاری میان ناتو و اتحادیه اروپا در حوزه‌هایی مثل حفاظت از زیرساخت‌های حیاتی خبر می‌دهد. بااین‌حال، برخلاف ناتو، اتحادیه اروپا حمایت و پشتیبانی فنی مستقیمی را در این حوزه فراهم نکرده است. از دیگر اختلافات مهم میان این دو گروه این است که اتحادیه اروپا نظام‌های اطلاعاتی کنترل و فرماندهی خاص خود را ندارد و فاقد نهاد مرکزی برای امنیت سایبر مشترک ـ همانند شورای آتلانتیک شمالی ـ است.

درمجموع، می‌توانیم دربارهٔ توان سایبری ناتو، نکات زیر را مورد تأکید قرار دهیم:

۱. به‌رغم اینکه کنفرانس سران ناتو در لیسبون خواهان ادغام ابعاد سایبری به دکترین ناتو بود، این فرایند به‌طور آهسته و نامتجانس صورت گرفته است. روابط میان فضای سایبری و عملیات‌های اطلاعاتی در دکترین ناتو نامشخص و تمرکز فضای سایبری در دکترین ناتو ماهیتاً دفاعی است.

۲. نقش فعالیت‌های فضای سایبری در عملیات‌های بازدارنده ناتو هنوز در هیچ مجمع عمومی‌ای تعریف نشده است.
۳. فضای سایبری در ناتو با چالش‌های پیچیده و درهم‌تنیده‌ای مثل حفاظت از زیرساخت‌های حیاتی در سطح ناتو و سطوح ملی مواجه است. بسیاری از کشورها در هماهنگی ادغام کردن رهیافت‌های ملی خود با چالش‌های بیشتری مواجه هستند.
۴. ناتو در ایجاد برنامه‌های آموزشی، تحصیلی و تمرینی در حوزه‌های سیاسی و نظامی مدیریت بحران در فضای سایبر موفق بوده است.
۵. ناتو دارای نقش قابل توجهی در صحنه جهانی در ایجاد استانداردها برای ارزیابی حقوقی فعالیت‌ها در فضای سایبر بوده است.
۶. فعالیت‌های سایبری ناتو نقش رهبری بی‌مانندی را برای برخی کشورهای کوچک در این اتحادیه فراهم نموده است.
۷. ناتو به‌خوبی توانسته است صنعت برخی کشورهای شریک و سازمان‌هایی مثل اتحادیه اروپا را در بسیاری از فعالیت‌های مرتبط به حوزه سایبر وارد نماید.
۸. تلاش‌ها برای کسب بودجه و منابع در حوزه سایبری در ناتو با دیگر حوزه‌های تخصیص بودجه (برای کارهای دیگر) در رقابت است.