

عصر ارتش‌های خودمختار و نبردهای الگوریتمی

ناصر کاوه

با همکاری هوش مصنوعی (Gemini)

Attributable Mass



Cost-Exchange Ratio



بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ

إِنَّمَا أَعْطَيْنَاكَ الْكَوْثَرَ (١) فَصَلِّ لِرَبِّكَ وَانْحَرْ (٢) إِنَّ شَانِئَكَ هُوَ الْأَبْتَرُ (٣)





این کتاب تقدیم می‌شود

"به ائمه معصومین (صلوات الله علیهم اجمعین)، امام خمینی (ره) و شهید خامنه ای، شهدا از صدر اسلام تا شهدای رمضان و هرمز"

کتاب «عصر ارتش‌های خودمختار و نبردهای الگوریتمی» پیش‌رو با یک واقعیت بنیادین آغاز می‌شود: نبردهای آینده پیش از آن‌که عرصه‌ای برای رقابت بر سر کالیبر آتش، برد موشک‌ها، توان انفجاری سرجنگی یا زره تانک‌ها باشند، در میدان تفوق الگوریتم‌ها رقم خواهند خورد؛ نبردی که در آن برتری به سامانه یا ارتشی تعلق می‌گیرد که بتواند داده‌های پراکنده را سریع‌تر گردآوری کند، آن را به درک عملیاتی بدل سازد و تصمیم را در کوتاه‌ترین زمان به اثرگذارهای میدانی ابلاغ نماید. در تاریخ نبردهای بشری، همواره تسلیحات به مثابه «ابزارهایی» مکانیکی یا الکترونیکی در ید اختیار فرمانده انسانی نگریسته می‌شدند؛ فرماندهی که در چارچوب یک زنجیره خطی مشخص، گزارش‌های واسطه از دیده‌بان‌ها را تحلیل می‌کرد و فرمان آتش را صادر می‌نمود.

«عصر ارتش‌های خودمختار و نبردهای الگوریتمی»

نویسنده : ناصرکاوه

هوش مصنوعی ، گرافیک و طراح : علی کربلانی

مشاور طرح ، رسانه و فضای مجازی : مهدی کاوه

ویراستار ، تایپ و حروف نگار : نرگس کاوه

روابط عمومی و پشتیبانی: فاطمه عاقلی

قیمت: صلوات بر محمد و آل محمد(ص)



زایش فرماندهی جنگ خودمختار (AutoWarCom)

وقتی ماشین از ابزارِ نبرد، به عاملِ مرگ و ترور تبدیل می‌شود.

گذر از عصر سلاح‌های تحت فرمان انسان، به عصر
عصر نبردهای الگوریتمی و عاملیت ماشین.

اعلامیه رسمی: تأسیس فرماندهی یکپارچه رزمی ۴
ستاره برای تسریع و تجميع سامانه‌های خودمختار.

فهرست مطالب

مقدمه/8

بخش اول: شالوده نهادی، دکترین ناصر کاوه و تکوین ارتش هفتم

فصل اول: فلسفه وجودی دکترین ناصر کاوه و چرخش پارادایم نبرد/11

فصل دوم: ارتش هفتم ایالات متحده و تبارشناسی فرماندهی جنگ خودمختار (AutoWarCom)/14

فصل سوم: پل مجتمع نظامی-فناورانه و بازیگران کلیدی/17

بخش دوم: کالبدشکافی فنی شبکه، همگرایی دامنه‌ها و هوش مصنوعی لبه

فصل چهارم: معماری دیدن، فهمیدن و عمل کردن (CJADC2 و Kill Web)/20

فصل پنجم: هوش مصنوعی لبه (Edge AI) و پلتفرم‌های ماژولار چنددامنه‌ای/24

بخش سوم: دینامیک ازدحام، کمیت فناورانه و پارادوکس اقتصاد نبرد

فصل ششم: پروژه رپلیکاتور (Replicator) و کمیت فناورانه مصرف‌پذیر/28

فصل هفتم: مدل‌سازی ریاضی نبرد و پارادوکس تبادل هزینه/32

بخش چهارم: انسان، عاملیت ماشینی و اخلاق نبرد الگوریتمی

فصل هشتم: طیف سه‌گانه نظارت و مسئله تأخیر مرگبار/36

فصل نهم: معماری مسئولیت، پاسخ‌گویی و توقف ایمن/40

بخش پنجم: کالبدشکافی ترورهای هدفمند؛ تکامل ۸۰ ساله و چهار بازوی نوین

فصل دهم: گاه‌شمار ۸۰ ساله ترور در دکترین امنیتی اسرائیل (۱۹۴۸ تا کنون)/47

فصل یازدهم: بازوهای چهارگانه ترورهای الگوریتمی مدرن/51

فصل دوازدهم: تمایز دستاورد تاکتیکی از پیروزی استراتژیک/55

بخش ششم: سناریوهای تهدید نامتقارن، تسلیحات غیردولتی و پیامدهای امنیتی

فصل سیزدهم: دموکراتیزه شدن تسلیحات خودمختار و بازیگران غیردولتی/58

فصل چهاردهم: پیامدهای راهبردی ترورهای خودمختار برای بازیگران دولتی/62

بخش هفتم: دکترین جامع پدافند؛ ایجاد کوری اطلاعاتی و تاب‌آوری چندلایه

فصل پانزدهم: پدافند علیه بینایی ماشین و حسگرهای خودمختار/66

فصل شانزدهم: مصون‌سازی زنجیره تأمین سخت‌افزار و پدافند شبکه‌ای/70

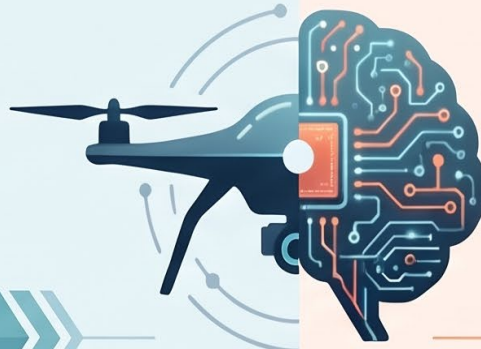
فصل هفدهم: تسلیحات انرژی هدایت‌شده، مسموم‌سازی داده‌ها و پدافند ازدحام/74

بخش هشتم: فرجام، روش‌شناسی اسناد و کتاب‌شناسی

موخره/78

سخن آخر/85

با همگرایی هوش مصنوعی لبه و پیهادهای خوداتکا، ماهیت نبرد از حالت انسان‌محور و پرهزینه به سوی «نبردهای الگوریتمی» تغییر یافته است. این فناوری انحصار قدرت نظامی را شکسته و همزمان در اختیار دولت‌ها جهت عملیات‌های نقطه‌زن و گروه‌های غیردولتی جهت نبردهای نامتقارن قرار گرفته است.



عصر ارتش‌های خودمختار: بازیگران دولتی در برابر غیردولتی

بازیگران دولتی (State Actors)



دقت جراحی و صفر کردن تلفات خودی

شناسایی اهداف با الگوریتم‌های هوشمند بدون نیاز به حضور فیزیکی نیرو در خاک دشمن.



دقت جراحی و صفر کردن تلفات خودی

شناسایی اهداف با الگوریتم‌های هوشمند بدون نیاز به حضور فیزیکی نیرو در خاک دشمن.



انکارپذیری موجه در عملیات راهبردی

بهره‌گیری از قطعات تجاری فاقد هویت برای رد مسئولیت و ابهام در انتساب حمله.



خطای الگوریتمی و تصاعد ناخواسته جنگ

خطر خطای مثبت کاذب در شناسایی هدف و تسریع غیرقابل کنترل تنش‌ها.

بازیگران غیردولتی (Non-State Actors)



دموکراتیزه شدن تسلیمات خودمختار

تلفیق پهپادهای تجاری ارزان قیمت با کدهای بینایی ماشین و هوش مصنوعی متن‌باز.



ایجاد تقارن شکنی و فلج روانی دشمن

دور زدن پدافندهای گران قیمت با ریزپرنده‌های ارزان و جایگزینی کد. مهارت نظامی.



ایجاد تقارن شکنی و فلج روانی دشمن

دور زدن پدافندهای گران قیمت با ریزپرنده‌های ارزان و جایگزینی کدنویسی با مهارت نظامی.



فقدان امکان لغو مأموریت پس از شلیک

قطع کامل پیوندهای ارتباطی برای فرار از اخلال و نبود دکمه توقف اضطراری.

مقدمه

از زنجیره فرمان تا شبکه تصمیم؛ چرخش پارادایم نبرد در عصر ماشین‌های هوشمند

کتاب پیش‌رو با یک واقعیت بنیادین آغاز می‌شود: نبردهای آینده پیش از آن‌که عرصه‌ای برای رقابت بر سر کالیبر آتش، برد موشک‌ها، توان انفجاری سرجنگی یا زره تانک‌ها باشند، در میدان تفوق الگوریتم‌ها رقم خواهند خورد؛ نبردی که در آن برتری به سامانه یا ارتشی تعلق می‌گیرد که بتواند داده‌های پراکنده را سریع‌تر گردآوری کند، آن را به درک عملیاتی بدل سازد و تصمیم را در کوتاه‌ترین زمان به اثرگذارهای میدانی ابلاغ نماید. در تاریخ نبردهای بشری، همواره تسلیحات به مثابه «ابزارهایی» مکانیکی یا الکترونیکی در ید اختیار فرمانده انسانی نگریسته می‌شدند؛ فرماندهی که در چارچوب یک زنجیره خطی مشخص، گزارش‌های واصله از دیده‌بان‌ها را تحلیل می‌کرد و فرمان آتش را صادر می‌نمود. اما معماری پیشنهادی «فرماندهی جنگ خودمختار» یا AutoWarCom که در کانون دکترین ناصر کاوه قرار دارد، این انگاره سنتی را دگرگون ساخته و فناوری را از موقعیت «ابزار در خدمت انسان» به تراز «عامل تصمیم‌گیر و سازمان‌دهنده صحنه نبرد» ارتقا داده است. در این پارادایم نوظهور، خط مستقیم فرماندهی که با عنوان چرخه کلاسیک OODA (مشاهده، جهت‌گیری، تصمیم و اقدام) شناخته می‌شد، در حال فروپاشی است. به جای این چرخه‌های کند و خطی، تازی چندمسیره، پویا و هم‌افزا با عنوان Kill Web (تار انهدام) شکل می‌گیرد که در آن حسگرهای فضایی، رادارهای آرایه‌فازی، پایشگرهای هوایی، پهپادها، شناورهای سطحی و حس

گروه‌های انفرادی به صورت لحظه‌ای با هم تبادل داده می‌کنند. این شبکه گسترده از طریق هوش مصنوعی لبه (Edge AI)، داده‌های حجیم را در نقطه‌ای نزدیک به صحنه پردازش کرده و فاصله کشف هدف تا اقدام عملیاتی را به چند ثانیه کاهش می‌دهد. در نتیجه این همگرایی، انحصار تصمیم‌گیری از قرارگاه‌های متمرکز خارج شده و به سیستم‌های توزیع‌شده محول می‌شود. با این حال، تعبیر «جنگ خودمختار» هرگز یک وضعیت دودویی و قطعی میان صفر و صد نیست؛ بلکه طیفی پیوسته از سامانه‌های تصمیم‌یار تا ماشین‌های با عاملیت بالا را شامل می‌شود.

هدف این کتاب آن است که بدون درغلتیدن به هیجان‌های ساختگی یا اغراق‌های ژورنالیستی، ابعاد فنی، نهادی، راهبردی و اخلاقی این تحول بی‌سابقه را موشکافی کند. از سویی، طرح‌هایی نظیر پروژه رپلیکاتور، پیوند پنتاگون با سیلیکون‌ولی از طریق واحد نوآوری دفاعی (DIU)، سامانه‌های هدف‌گیری الگوریتمی و بهره‌گیری از هوش مصنوعی در ترورهای پیچیده بررسی می‌شوند؛ و از سوی دیگر، پیامدهای اقتصادی دکترین کمیت مصرف‌پذیر، خطرات خروج شتابزده انسان از حلقه نظارت، آسیب‌پذیری‌های سایبری، جعل بینایی ماشین و مخاطرات دستیابی بازیگران غیردولتی به تسلیحات ارزان و خودمختار تشریح می‌گردند.

در نهایت، این اثر روایتی است سنجیده از گذار نبردها از ساحت اراده صرف انسانی به هندسه شبکه‌های الگوریتمی؛ روایتی برای تصمیم‌سازان و مدافعانی که دریافته‌اند در جهان فردا، کوری در برابر زبان داده‌ها، به معنای خلع‌سلاح مطلق پیش از شلیک نخستین گلوله خواهد بود.

عصر ارتش‌های خودمختار و نبردهای الگوریتمی

ناصر کاوه

با همکاری هوش مصنوعی (Gemini)



بخش اول: شالوده نهادی، تکوین ارتش هفتم

فصل اول: فلسفه وجودی دکترین ناصر کاوه و چرخش پارادایم نبرد

(گذار از ابزار به عامل و بازتعریف زمان در جنگ)

دکترین فرماندهی جنگ خودمختار (AutoWarCom) که توسط ناصر کاوه صورت‌بندی شده است، تنها یک نظریه پیرامون نوسازی تجهیزات نظامی نیست، بلکه نمایانگر یک «گسست معرفت‌شناختی» در تاریخ جنگ‌های بشری است. در تمام طول تاریخ، از اختراع باروت تا توسعه جنگنده‌های نسل پنجم، فناوری همواره در قالب «ابزار کمکی» (Auxiliary Tool) در خدمت اراده انسان عمل کرده است. در این پارادایم سنتی، یک تانک یا موشک کروز، هر قدر هم که پیشرفته باشد، بدون دریافت فرمان مستقیم اپراتور انسانی ماهیتی خنثی دارد. اما دکترین کاوه بر این واقعیت استوار است که با ظهور الگوریتم‌های یادگیری ماشین و هوش مصنوعی، فناوری از جایگاه ابزار تنزل‌یافته خارج شده و به مقام «عامل» (Agent) و «سازمان‌دهنده» میدان نبرد ارتقا یافته است. در این ساحت نوین، ماشین‌ها دیگر منتظر فرمان شلیک نمی‌مانند، بلکه خود بر اساس داده‌های محیطی، اهداف را شناسایی، اولویت‌بندی و منهدم می‌کنند. این چرخش پارادایم، مستلزم بازتعریف بنیادین مفهوم «فرماندهی» است. در جنگ‌های کلاسیک، فرماندهی به معنای مدیریت خطی نیروها و صدور فرامین تاکتیکی بود. اما در عصر تراشه‌ها و پردازش‌های کوانتومی، پدیده‌ای به نام «فشرده‌سازی زمان» (Time " " Compression) رخ داده است. زمان

واکنش و شناخت انسان (Human Cognition) در مقیاس ثانیه و دقیقه عمل می‌کند، در حالی که الگوریتم‌های هوش مصنوعی لبه (Edge AI) محیط را در مقیاس میلی‌ثانیه پردازش و تحلیل می‌کنند: $\Delta t_{\text{Human}} \ll \Delta t_{\text{Algorithmic}}$. وقتی یک سامانه پدافندی خودمختار یا ازدحام پهبادی با سرعت نور با یکدیگر تبادل داده می‌کنند، حضور انسان در حلقه تصمیم‌گیری تاکتیکی (Human-in-the-loop) نه تنها مفید نیست، بلکه به یک «تأخیر مرگبار» و نقطه ضعف استراتژیک بدل می‌شود. در دکترین ناصر کاوه، نقش فرمانده از یک «مدیر خرد تاکتیکی» به یک «معمار الگوریتم و استراتژیست» تغییر می‌یابد. فرمانده فردا کسی است که پارامترهای اولیه، مرزهای اخلاقی درگیری و قواعد بازی (Rules of Engagement) را برای شبکه ماشین‌ها تعریف می‌کند و سپس اجرای آن را به تار کشتار (Kill Web) می‌سپارد. با توجه به پیچیدگی و ابعاد حیرت‌انگیز این تحول، روش‌شناسی این اثر مبتنی بر تفکیک دقیق چهار سطح تحلیلی است: نخست، «واقعیت‌های اثبات‌شده میدانی» نظیر استفاده فعلی از پهپادهای کامیکازه و سامانه‌های پردازش تصویر در جنگ‌های اخیر؛ دوم، «اسناد سازمانی و بودجه‌ای» که نشان‌دهنده جهت‌گیری نهادهای نظامی (مانند پنتاگون و ارتش اسرائیل) است؛ سوم، «پیشنهادهای معماری» که در قالب دکترین AutoWarCom برای یکپارچه‌سازی این سامانه‌ها ارائه می‌شود؛ و چهارم، «سناریوهای آینده‌پژوهانه» که وضعیت جنگ‌ها را در افق ۲۰۳۰ و فراتر از آن ترسیم می‌کند. این تفکیک روش‌شناختی به خواننده اجازه می‌دهد تا میان داستان‌های علمی-تخیلی با واقعیت‌های مهلک و قریب‌الوقوع نظامی تمایز قائل شود و درک کند که جنگ خودمختار نه یک ایده برای آینده دور، بلکه واقعیتی در حال تکوین در لحظه حال است.

عصر ارتش‌های خودمختار و نبردهای الگوریتمی

مبتنی بر دکترین و معماری ناصر کاوه (AutoWarCom)

با همکاری هوش مصنوعی (Gemini)



فصل دوم: ارتش هفتم ایالات متحده و تبارشناسی فرماندهی جنگ خودمختار (AutoWarCom)

(خروج از جزایر سازمانی و چالش‌های معماری نوین)

برای درک چگونگی نهادینه شدن دکترین جنگ خودمختار، مطالعه روند دگرپرسی در ساختارهای نظامی، به ویژه در نیروهای مسلح ایالات متحده، ضروری است. مفهوم «ارتش هفتم» در ادبیات کلاسیک نظامی آمریکا به نیروهای مستقر در اروپا (USAREUR) و تجارب تاریخی دوران جنگ سرد و جنگ جهانی دوم ارجاع دارد؛ اما در ادبیات و تبارشناسی نوین نبردهای الگوریتمی، این مفهوم استعاره‌ای از تجمع نیروها و تبدیل ساختارهای سنگین و سنتی به شبکه‌های چابک و خودمختار است. ارتش‌ها همواره بر پایه تفکیک حوزه‌های عملیاتی (زمین، هوا، دریا) سازمان‌دهی شده‌اند. اما جنگ خودمختار نیازمند بستری است که در آن تمایز این دامنه‌ها از بین برود.

در معماری پیشنهادی دکترین کاوه، فرماندهی جنگ خودمختار (AutoWarCom) نباید به عنوان یک زیربخش کوچک در نیروی هوایی یا زمینی تعریف شود، بلکه باید جایگاهی هم‌تراز با فرماندهی‌های رزمی چهارستاره و مستقل ایالات متحده نظیر فرماندهی عملیات ویژه (USSOCOM) یا فرماندهی سایبری (USCYBERCOM) داشته باشد. دلیل این امر روشن است: یک پهباد خودمختار ممکن است داده‌های هدفیابی خود را از یک حسگر فضایی دریافت کند، از پوشش جنگال یک یگان دریایی بهره‌برد و هم‌زمان با نفوذ سایبری به شبکه راداری دشمن هماهنگ شود. این سطح از همگرایی نیازمند خروج سامانه‌ها از «جزایر سازمانی» (Organizational Silos) است.

در ساختار سنتی، نیروی دریایی دیتاسنترها و استانداردهای ارتباطی خاص خود را دارد و نیروی هوایی نیز پروتکل‌های مجزایی را دنبال می‌کند. AutoWarCom به عنوان یک نهاد فرادامنه، این دیوارهای بوروکراتیک را در هم می‌شکند و یک شبکه عصبی واحد برای کل ارتش ایجاد می‌کند.

با این وجود، بررسی انتقادی این ادعا در اسناد نشان می‌دهد که تأسیس یک فرماندهی مستقل خودمختار با موانع ساختاری، حقوقی و بودجه‌ای عظیمی روبرو است.

از منظر حقوقی و اختیارات مبتنی بر «عنوان ۱۰ مجموعه قوانین ایالات متحده» (Title 10 Authorities)، نیروهای مسلح سنتی (مانند ارتش یا نیروی هوایی) به شدت در برابر واگذاری بودجه‌های کلان و پرسنل متخصص خود به یک فرماندهی جدید مقاومت می‌کنند. علاوه بر رقابت‌های بین‌سرویسی (Inter-service Rivalry)، کنگره نیز در تخصیص بودجه‌های ده‌ها میلیارد دلاری برای سیستم‌هایی که ماهیت آن‌ها «مصرف‌پذیر» (Attritable) و فاقد خلبان است، با تردیدهای جدی مواجه است؛ چرا که چرخه اقتصاد سیاسی آمریکا با پیمانکاران بزرگ اسلحه‌سازی (مانند لاکهید مارتین که پلتفرم‌های گران‌قیمت می‌سازند) پیوند خورده است. از این رو، ارتش هفتم نوین و AutoWarCom پیش از آنکه با دشمنان خارجی بجنگند، باید در جبهه داخلی با بوروکراسی کند و ساختارهای سنتی بودجه‌ریزی مبارزه کنند تا بتوانند گذار به عصر نبردهای چنددامنه‌ای یکپارچه را محقق سازند.

«عصر ارتش‌های خودمختار و نبردهای الگوریتمی»

ناصر کاوه با همکاری هوش مصنوعی (Gemini)



فصل سوم: پل مجتمع نظامی-فناورانه و بازیگران کلیدی

(ادغام سیلیکون‌ولی در ماشین جنگ و افق ۲۰۲۷)

مهم‌ترین وجه تمایز انقلاب نظامی کنونی (جنگ خودمختار) با انقلاب‌های پیشین در این است که مرکز ثقل نوآوری از آزمایشگاه‌های دولتی و نظامی (نظیر DARPA یا لس‌آلاموس در دوران جنگ سرد) به بخش تجاری و شرکت‌های فناوری اطلاعات در سیلیکون‌ولی منتقل شده است. فصل سوم دکترین ناصر کاوه، کالبدشکافی این «پل مجتمع نظامی-فناورانه» (Military-Tech Complex) است. ساخت و توسعه هوش مصنوعی پیشرفته، پردازش ابری و الگوریتم‌های بینایی ماشین دیگر در انحصار ژنرال‌های نظامی نیست؛ بلکه در دست شرکت‌هایی نظیر گوگل، مایکروسافت، آمازون و استارت‌آپ‌های ساختارشکن مانند آندوریل (Anduril) و پالانتیر (Palantir) قرار دارد. در این میان، پروژه‌های زمان‌بندی‌شده نقش کاتالیزور را ایفا می‌کنند. «پروژه آگینکورت» (Agincourt) با تعیین افق هدف ۱ اکتبر ۲۰۲۷، به وضوح نشان‌دهنده شتاب هیجانی پنتاگون برای آماده‌سازی ساختارها در برابر تهدیدات نامتقارن و احتمال درگیری‌های بزرگ در حوزه اقیانوس آرام (نظیر سناریوی تایوان) است. برای تحقق این ضرب‌الاجل، نیازمند چهره‌هایی هستیم که زبان مشترک میان کدهای سیلیکون‌ولی و نیازهای خشن میدان نبرد را درک کنند. افرادی نظیر «اوون وست» (Owen West) در جایگاه استراتژیست‌های نوآوری دفاعی و «مکس استراسایزر» (Max Strausizer) با تجربه تلفیق نیازهای میدانی با قابلیت‌های نرم‌افزاری، به عنوان مفصل‌های اتصال این دو

جهان متفاوت عمل کرده‌اند. آن‌ها می‌دانند که یک سرباز در محیط فاقد ارتباطات (GPS-Denied) به چه نوع هوش مصنوعی محلی و کم‌مصرفی نیاز دارد.

نهاد کلیدی در این پیوند، «واحد نوآوری دفاعی» (DIU - Defense Innovation Unit) است؛ دفتری که پنتاگون مستقیماً در قالب سیلیکون‌ولی تأسیس کرد تا چرخه‌های ده ساله خرید تسلیحات را دور زده و قراردادهای نرم‌افزاری را در کمتر از شش ماه با استارت‌آپ‌های تجاری منعقد کند. DIU توانست فرهنگ چابک استارت‌آپی را به ارتش تزریق کند. اما هیچ‌یک از این الگوریتم‌ها بدون زیرساخت داده کارآمد عملیاتی نمی‌شوند. «زیرساخت داده‌های ابری مشترک نظامی» (JWCC)، قراردادی ۹ میلیارد دلاری با غول‌های فناوری (آمازون، گوگل، مایکروسافت، اوراکل)، ستون فقرات AutoWarCom است. پروژه‌هایی نظیر «پروژه میون» (Project Maven) که در ابتدا برای پردازش هوشمند تصاویر پهپادها با استفاده از هوش مصنوعی گوگل توسعه یافت و «پروژه نیمبوس» (Project Nimbus) که فضای ابری یکپارچه و امنی را برای نیروهای مسلح فراهم می‌سازد، پایه‌های این پل هستند. ادغام این توان تجاری (Big Tech) در ساختار جنگ خودمختار، نشان می‌دهد که در جنگ‌های آینده، پیروزی نه در خطوط مونتاژ تانک‌ها، بلکه در سرورهای ابری، دیتاسنترها و خطوط کدی رقم می‌خورد که توسط مهندسان نرم‌افزار غیرنظامی در کالیفرنیا یا تل‌آویو توسعه یافته‌اند. این پیوند تجاری-نظامی، ماهیت جنگ را به پدیده‌ای کاملاً داده‌محور و الگوریتم‌بنیان تبدیل کرده است.

عصر ارتش‌های خودمختار و نبردهای الگوریتمی

ناصر کاوه

با همکاری هوش مصنوعی (Gemini)



بخش دوم: کالبدشکافی فنی شبکه، همگرایی دامنه‌ها و هوش مصنوعی لبه

فصل چهارم: معماری دیدن، فهمیدن و عمل کردن (CJADC2 و Kill Web)

(گذار از ساختارهای خطی به شبکه‌های ارگانیک نبرد)

در قلب دکترین فرماندهی جنگ خودمختار (AutoWarCom)، سه‌گانه «دیدن، فهمیدن و عمل کردن» قرار دارد که معادل مدرن و ماشین‌محور چرخه کلاسیک تصمیم‌گیری است. برای تحقق این سه‌گانه در مقیاس همه‌جانبه، پنتاگون و نظریه‌پردازان نظامی به سوی معماری نوینی تحت عنوان «سامانه فرماندهی و کنترل یکپارچه همه دامنه‌ها» (CJADC2) حرکت کرده‌اند. CJADC2 تنها یک نرم‌افزار یا شبکه ارتباطی نیست، بلکه یک «فلسفه سایبرنتیک» است. در این معماری، اطلاعات به‌دست‌آمده از حسگرهای فضایی (ماهواره‌ها)، هوایی (آواکس‌ها و پهپادها)، دریایی (سونارها و رادارها)، زمینی و حتی سایبری، در یک بستر ابری مشترک ترکیب می‌شوند. این بدان معناست که یک ناو مستقر در اقیانوس آرام می‌تواند موشک خود را بر اساس مختصات شلیک کند که توسط یک جنگنده پنهان‌کار یا یک ریزپرنده در صدها کیلومتر دورتر به دست آمده است. CJADC2 مرزهای سنتی میان نیروهای مسلح را از بین برده و کل ارتش را به یک ارگانیزم واحد و واکنش‌گر تبدیل می‌کند.

با استقرار این سیستم، یکی از بزرگ‌ترین دگرگونی‌های تاکتیکی تاریخ رخ می‌دهد: جایگزینی «زنجیره خطی کشتار» (Kill " " Chain) با «تار انهدام چندمسیره» (Kill " " Web). زنجیره کشتار کلاسیک، فرایندی متوالی و شکننده شامل مراحل یافتن، تثبیت، رهگیری، هدف‌گیری، درگیری و ارزیابی (F2T2EA) بود.

ضعف بنیادی زنجیره در نام آن نهفته است؛ اگر یک حلقه از این زنجیر (مثلاً رادار رهگیر یا پل ارتباطی) منهدم یا مختل شود، کل فرایند از کار می‌افتد. اما در مفهوم «تار انهدام»، ساختار شبکه شبیه به تار عنکبوت یا گراف‌های غیرمتمرکز است.

اگر یک گره ارتباطی یا یک سکوی پرتاب از بین برود، هوش مصنوعی بلافاصله و در کسری از ثانیه، مسیر جدیدی برای جریان داده و شلیک جایگزین پیدا می‌کند. این ویژگی، تاب‌آوری (Resilience) شبکه را به شدت در برابر حملات دشمن افزایش می‌دهد.

نتیجه بلافاصل این معماری، کاهش حیرت‌انگیز فاصله «حسگر تا تیرانداز» (Sensor-"-" to-"-" Shooter) است. در طول جنگ خلیج فارس، هفته‌ها و روزها طول می‌کشید تا تصاویر ماهواره‌ای تحلیل شده، اهداف انتخاب گردند و دستور شلیک به خلبان ابلاغ شود.

امروزه در دکترین AutoWarCom، الگوریتم‌های پردازش تصویر در لحظه هدف را می‌بینند، با پایگاه داده تطبیق می‌دهند و مختصات را به نزدیک‌ترین و مناسب‌ترین سلاح ارسال می‌کنند.

این زمان از هفته و روز، ابتدا به دقیقه و اکنون به چند ثانیه کاهش یافته است. سرعت این چرخه به قدری بالاست که دشمن انسانی عملاً فرصت پنهان شدن یا واکنش متقابل را از دست می‌دهد.

با این وجود، معماری CJADC2 با چالش‌های مرگبار و پیچیده‌ای در حوزه جریان داده روبه‌رو است. نخستین چالش، «احراز هویت پیوسته» در شبکه‌ای است که روزانه میلیاردها بسته داده در آن تبادل می‌شود. اگر شبکه نتواند در کسری از ثانیه اصالت یک داده را تأیید کند، دشمن می‌تواند با تکنیک‌های جعل، اطلاعات دروغین را وارد تار انهدام کند. دومین چالش، خطر «داده‌های آلوده» (Data " " Poisoning) است؛ جایی که حریف با دستکاری‌های ظریف در محیط یا امواج الکترومغناطیس، الگوریتم‌های یادگیری ماشین را فریب می‌دهد تا یک اتوبوس مسافربری را به عنوان یک پرتابگر موشک شناسایی کنند.

اما ترسناک‌ترین چالش، «تکثیر نمایی خطای الگوریتمی» (Exponential " " Multiplication" " of" " Errors) است.

در یک شبکه به هم پیوسته خودمختار، یک خطای کوچک در یک حسگر محلی (مثلاً تشخیص اشتباه یک هدف) می‌تواند با سرعت نور در کل شبکه بازنشر شده و منجر به واکنش‌های زنجیره‌ای و شلیک‌های ناخواسته در مقیاس وسیع شود.

به همین دلیل، مدیریت بار شناختی و کنترل کیفیت داده‌ها، حیاتی‌ترین بخش در پدافند سایبری AutoWarCom محسوب می‌شود.

عصر ارتش‌های خودمختار و نبردهای الگوریتمی

ناصر کاوه

با همکاری هوش مصنوعی (Gemini)

طرح مفهومی پروژۀ در ریپلیکاتور



مقایسه ظرفیت‌ها

Attritable Mass



هزاران واحد ارزان قیمت و قابل جایگزینی

Cost-Exchange Ratio



هزینه بالا در برابر
تلفات گسترده در مقیاس انبوه

فصل پنجم: هوش مصنوعی لبه (Edge AI) و پلتفرم‌های ماژولار چنددامنه‌ای

(استقلال تاکتیکی در محیط‌های کور و جنگال‌زده)

مفهوم «هوش مصنوعی لبه» (Edge " " AI) پاسخی است به یکی از بزرگ‌ترین آسیب‌پذیری‌های شبکه‌های نظامی متمرکز: وابستگی مطلق به ارتباطات ماهواره‌ای و سرورهای ابری راه دور.

در نبردهای مدرن، ارسال تمام ویدئوها و داده‌های حسگری هزاران پهپاد به یک دیتاسنتر مرکزی برای پردازش، نیازمند پهنای باند عظیمی است که در میدان جنگ به راحتی توسط دشمن کشف، مختل یا شنود می‌شود.

علاوه بر این، تأخیر زمانی (Latency) ناشی از رفت‌وبرگشت سیگنال‌ها، می‌تواند به قیمت از دست رفتن یک هدف متحرک تمام شود. دکتربین ناصر کاوه بر این اصل تأکید دارد که قدرت پردازش، باید به «لبه شبکه»، یعنی دقیقاً روی پردازنده‌های نصب‌شده در پهپادها، ریزپردازنده‌ها و موشک‌ها منتقل شود.

با استفاده از میکروچیپ‌های کم‌مصرف و قدرتمند، پلتفرم‌ها به جای ارسال داده‌های خام، خودشان داده‌ها را تحلیل کرده و تنها «نتیجه پردازش» (مثلاً: «هدف الف در مختصات ب رؤیت شد») را در قالب چند بایت اطلاعات ارسال می‌کنند.

این امر، پردازش نامتمرکز را محقق کرده و وابستگی به پهنای باند را به شدت کاهش می‌دهد.

اهمیت Edge AI زمانی به اوج خود می‌رسد که پلتفرم‌های خودمختار وارد محیط‌های فاقد جی‌پی‌اس (" Denied"-" GPS Environments) می‌شوند. در هر نبرد تقارنی یا نامتقارن، نخستین اقدام مدافع، ایجاد اختلال وسیع (Jamming) در سیگنال‌های ناوبری ماهواره‌ای (GPS/GNSS) است. سیستم‌هایی که صرفاً متکی به این سیگنال‌ها باشند، بلافاصله فلج شده و سقوط می‌کنند.

برای عبور از این سد، AutoWarCom به سیستم‌های ناوبری مبتنی بر بینایی ماشین و همجوئی حسگرها روی آورده است. تکنیک «مکان‌یابی و نقشه‌برداری همزمان بصری» (Visual " " SLAM) به پرنده اجازه می‌دهد تا از طریق دوربین‌های خود، هندسه سه‌بعدی محیط (مانند ساختمان‌ها، خیابان‌ها و درختان) را ببیند، نقشه‌ای از آن بسازد و موقعیت خود را درون این نقشه استنتاج کند.

در کنار آن، سامانه‌های «انطباق عوارض زمینی» (TERCOM) با استفاده از رادارهای ارتفاع‌سنج، توپوگرافی زمین زیر پای خود را با نقشه‌های از پیش ذخیره‌شده در حافظه تطبیق می‌دهند و مسیر را بدون نیاز به هیچ‌گونه سیگنال خارجی اصلاح می‌کنند. اما یک پلتفرم خودمختار برای اجرای عملیات گروهی (Swarming) همچنان نیازمند ارتباط با سایر گره‌هاست. در شرایطی که امواج رادیویی (RF) تحت اختلال شدید جنگ الکترونیک (EW) قرار دارند، اتکای شبکه به سوی «پیوندهای نوری و لیزری» (" Optical" " Space"-" Free Communication) معطوف می‌شود.

ارتباطات لیزری به دلیل استفاده از پرتوهای بسیار باریک و جهت‌دار، تقریباً غیرقابل شنود و غیرقابل اخلاص توسط جمرهای رادیویی هستند. این پیوندهای نوری که با رمزنگاری مقاوم سخت‌افزاری (و در آینده رمزنگاری کوانتومی) محافظت می‌شوند، تاب‌آوری شبکه تبادل داده را در خصمانه‌ترین محیط‌های الکترومغناطیسی تضمین می‌کنند.

بر بستر این هوش لیه و ارتباطات مقاوم، دکترین AutoWarCom نسل جدیدی از سلاح‌ها را با عنوان «پلتفرم‌های چنددامنه‌ای مصرف‌پذیر» (Attritable "Platforms") وارد میدان می‌کند. دوران تکیه مطلق بر جنگنده‌های چندصد میلیون دلاری یا ناوهای هواپیمابر غول‌پیکر رو به پایان است. این تجهیزات کلاسیک در برابر موشک‌های هایپرسونیک و ازدحام رباتیک بسیار آسیب‌پذیرند. به جای آن‌ها، ارتش خودمختار متکی به توده‌های انبوهی از سیستم‌های ارزان، ماژولار و مصرف‌پذیر است: ریزپرنده‌های انتحاری که فضای شهری را پاکسازی می‌کنند، پهپادهای شناسایی، شهپادها (شناورهای هدایت‌پذیر از دور سطحی) که بنادر را مین‌گذاری می‌کنند، زیردریایی‌های بدون سرنشین و خودروهای خودمختار زرهی. این پلتفرم‌ها به‌گونه‌ای طراحی شده‌اند که اگر ۵۰ درصد از آن‌ها در مسیر رسیدن به هدف نابود شوند، مأموریت همچنان با موفقیت توسط واحدهای باقی‌مانده که از طریق Edge AI بازآرایی شده‌اند، به انجام برسد. این تغییر نگرش از «کیفیت و بقای تک‌واحدی» به سوی «کمیت هوشمند و بقای شبکه‌ای»، جوهره کالبدشکافی فنی شبکه در جنگ‌های آینده است.

عصر ارتش‌های خودمختار و نبردهای الگوریتمی

اثر ناصر کاوه با همکاری هوش مصنوعی Gemini

شبکه‌سازی جهانی
اتصال یامرار
و تاب‌آوری بالا

- مهاوربها
- مهاوربها
- کپی‌بها
- رابط‌های زمینی
- گره‌های ارتباطی

توبواوزی شبکه



- گره‌های اصلی
- گره‌های فرعی
- مسیرهای ارتباطی
- پیش‌بینی‌های جابجایی
- مقاومت در برابر اختلال

پروژه نکتیرکننده

REPLICATOR



هزاران باقی‌مانده
یک مهمی مشترک



- بهبادهای خودمختار
- شنورهای بدون سرنشین
- رابط‌های زمینی
- همه در یک شبکه
- هوشمند و هماهنگ

مقایسه اتراق‌پذیری و هزینه

مؤرخه ابتدایان یلویز



بهره‌دهنده > 10,000



شنورهای > 1,000



رابط‌های زمینی

بهره‌دهنده > 500

نسبت جایگزینی مؤرخه



بهره‌دهنده 1:10



شنورهای 1:20



رابط‌های زمینی

1:15

بیشتر، ارزان‌تر، مقاومت



- تراکم بالا
- هماهنگی هوشمند
- یادگیری جمعی
- تصمیم‌گیری توزیع‌شده
- عملیات مسافت

هزاران واحد ← یک مغز ← یک اراده

قدرت در انبوهی است که هوشمندانه عمل می‌کند



هوش
مصنوعی



شبکه‌های توزیع‌شده



پایداری و
انعطاف‌پذیری

بخش سوم: دینامیک ازدحام، کمیت فناوریانه و پارادوکس اقتصاد نبرد

فصل ششم: پروژه رپلیکاتور (Replicator) و کمیت فناوریانه مصرف‌پذیر

(پایان عصر پلتفرم‌های طلایی و ظهور توده‌های هوشمند)

یکی از بنیادی‌ترین تغییرات راهبردی در دکترین فرماندهی جنگ خودمختار (AutoWarCom)، تغییر رویکرد از «کیفیت متمرکز» به «کمیت ارزان، هوشمند و توزیع‌شده» است.

برای دهه‌ها، ارتش‌های کلاسیک (به‌ویژه بلوک غرب) بر توسعه پلتفرم‌های فوق‌پیشرفته، رادارگریز و بی‌نهایت گران‌قیمت (موسوم به Exquisite Platforms) مانند جنگنده‌های اف-۳۵، بمب‌افکن‌های استراتژیک و ناوهای هواپیمابر تکیه داشتند.

این تجهیزات، اگرچه از نظر فناوری در قله قرار دارند، اما دارای یک نقطه‌ضعف کشنده هستند: زمان طولانی تولید و هزینه نجومی جایگزینی.

از دست دادن حتی یکی از این دارایی‌ها در میدان نبرد، یک فاجعه ملی و استراتژیک محسوب می‌شود. در پاسخ به این شکنندگی ساختاری، پنتاگون «پروژه رپلیکاتور» (Replicator) را معرفی کرد؛ پروژه‌ای که هدف آن تولید و استقرار ده‌ها هزار سیستم بدون سرنشین و خودمختار در زمین، هوا و دریا در بازه زمانی کوتاه (۱۸ تا ۲۴ ماه) است.

هدف رپلیکاتور، غلبه بر مزیت کمی دشمن از طریق ایجاد یک «کمیت فناورانه مصرف‌پذیر» (Attritable " " Mass) است.

مفهوم «دارایی مصرف‌پذیر» (Attritable) در ادبیات نظامی نوین به معنای بی‌ارزش بودن سلاح نیست، بلکه به سیستم‌هایی اطلاق می‌شود که هزینه تولید آن‌ها به قدری پایین است که فرمانده می‌تواند آن‌ها را در مأموریت‌های پرخطر با احتمال نابودی بالا (نظیر نفوذ به لایه‌های پدافندی متراکم دشمن) فدا کند، بدون آنکه موازنه قدرت نظامی یا بودجه دفاعی کشور دچار فروپاشی شود. تحقق این امر نیازمند یک انقلاب در منطق تولید و زنجیره‌های تأمین است.

در این پارادایم، ارتش‌ها دیگر نمی‌توانند به کارخانه‌های کند و انحصاری پیمانکاران سنتی دفاعی وابسته بمانند. تولید ده‌ها هزار پهپاد در ماه، مستلزم بهره‌گیری از خطوط تولید تجاری، استفاده از قطعات الکترونیکی با استاندارد غیرنظامی (COTS: Commercial Off-The-Shelf)، چاپ سه‌بعدی بدنه پلتفرم‌ها و بهره‌گیری از موتورها و باتری‌های موجود در بازار آزاد است.

این تغییر مقیاس، لجستیک جنگ را از یک «لجستیک نقطه‌ای» به یک «لجستیک توزیع‌شده و انعطاف‌پذیر» تبدیل می‌کند. هنگامی که این کمیت عظیم تولید شد، نیازمند یک ساختار فرماندهی شبکه‌ای است که در قالب «ازدحام خودمختار» (Autonomous " " Swarm) تجلی می‌یابد. یک ازدحام، صرفاً پرواز همزمان صدها پهپاد نیست (مانند حملات کلاسیک کروزها)؛ بلکه یک ارگانیزم زنده و سایبرنتیک است که از قوانین رفتار جمعی (Biomimicry) در طبیعت، نظیر حرکت دسته‌جمعی پرندگان یا ماهی‌ها، الهام گرفته است.

در یک Swarm، پهپادها با استفاده از هوش مصنوعی لبه (Edge AI) و بدون نیاز به هدایت مرکزی انسان، دائماً در حال تبادل موقعیت، سرعت و اهداف خود با یکدیگر هستند. این معماری، تاب‌آوری توپولوژیک (Topological " " Resilience) شگفت‌انگیزی به شبکه می‌بخشد. اگر سیستم‌های پدافندی دشمن ۵۰ درصد از پهپادهای یک ازدحام را در مسیر سرنگون کنند، گره‌های بازمانده در کسری از ثانیه شبکه را بازسازی کرده (Self-" " Healing)، نقش‌ها را میان خود بازتوزیع نموده و با حفظ انسجام، به سوی هدف نهایی هجوم می‌برند.

در این حالت، نابودی فیزیکی واحدها منجر به فروپاشی مأموریت نمی‌شود، زیرا «هوش» در کل توده پخش شده است و هیچ نقطه شکست واحدی (Single " " Point " " of " " Failure) وجود ندارد.

عصر ارتش‌های خودمختار و نبردهای الگوریتمی



ناصر کاوه
با همکاری هوش مصنوعی (Gemini)

فصل هفتم: مدل‌سازی ریاضی نبرد و پارادوکس تبادل هزینه

(چگونه اقتصاد پدافند را به زانو درآوریم؟)

ورود ازدحام‌های خودمختار و سامانه‌های ارزان‌قیمت به میدان نبرد، معادلات کلاسیک و مدل‌سازی‌های ریاضی جنگ را به طور بنیادین دگرگون کرده است. از جنگ جهانی اول تاکنون، استراتژیست‌های نظامی برای محاسبه نرخ تلفات و پیش‌بینی نتیجه نبرد از «معادلات لانچستر» (Lanchester's Laws) استفاده می‌کردند.

قانون مربع لانچستر (Lanchester's Square Law) نشان می‌دهد که قدرت یک نیروی نظامی، متناسب با «مجذور» تعداد واحدهای آن است؛ به این معنا که تمرکز نیرو و شلیک متمرکز، کلید پیروزی در جنگ‌های متقارن است.

اما در دکترین AutoWarCom، پلتفرم‌های توزیع‌شده و الگوریتم‌های هوش مصنوعی با تغییر ضریب اثربخشی (Efficiency Coefficient)، این معادلات خطی را ناکارآمد می‌کنند. یک ازدحام غیرمتمرکز از پهپادهای کامیکازه، نیازی به تمرکز فیزیکی در یک نقطه ندارد، بلکه با ایجاد یک شبکه محاصره‌کننده (Envelope) از جهات و ارتفاعات مختلف، دفاع خطی حریف را دور می‌زند.

علاوه بر ناکارآمدی مدل‌های فرسایش کلاسیک، مهم‌ترین بحران برای یک نیروی مدافع در عصر حاضر، «پارادوکس تبادل هزینه» (Cost-" Exchange" " Paradox) است. ارتش‌های مدرن برای حفاظت از خود، سامانه‌های پدافند هوایی لایه‌ای (مانند پاتریوت، گنبد آهنین یا ایجیس) را با هزینه‌هایی سرسام‌آور توسعه داده‌اند. این سامانه‌ها برای مقابله با جنگنده‌ها و موشک‌های بالستیک طراحی شده‌اند، نه برای رهگیری هزاران ریزپرنده ارزان‌قیمت. در این شرایط، ریاضیات اقتصاد نبرد با یک نابرابری کشنده مواجه می‌شود که با فرمول زیر قابل تبیین است:

$$\text{Cost-" Exchange" " Ratio} = C_{\text{int}}/C_{\text{att}} \gg 1$$

در این معادله، C_{int} نمایانگر هزینه رهگیری (Cost" " of" " Interception) شامل قیمت موشک پدافندی، استهلاک رادار و هزینه‌های عملیاتی است. در مقابل، C_{att} نشان‌دهنده هزینه پرتابه مهاجم (Cost" " of" " Attacker) نظیر یک پهپاد شاهد یا یک کوادکوپتر مسلح است. وقتی یک موشک پدافندی ۳ میلیون دلاری (مانند SM-2 یا پاتریوت) برای انهدام یک پهپاد ۲۰ هزار دلاری شلیک می‌شود، نسبت تبادل هزینه به شدت به ضرر مدافع (بزرگتر از یک و گاهی با ضریب ۱۰۰) خواهد بود.

استراتژیست‌های جنگ خودمختار از این فرمول نه صرفاً برای انهدام فیزیکی هدف، بلکه به عنوان سلاحی برای «فرسایش مالی و ورشکستگی اقتصادی» دشمن استفاده می‌کنند. حریف حتی اگر ۱۰۰ درصد حملات را با موفقیت رهگیری کند، در یک نبرد فرسایشی چندماهه، بودجه دفاعی و ذخایر موشک‌های استراتژیک خود را به اتمام خواهد رساند.

پیامد دیگر این حملات نامتقارن و پرتعداد، ایجاد پدیده «اشباع سیستمی و فرسودگی راداری» (Radar " " Fatigue" "&" " Saturation) است. رادارهای پیشرفته آرایه فازی (AESA) دارای محدودیت در تعداد فایل‌های رهگیری همزمان (Track " " Files) هستند. هنگامی که یک ازدحام چند صد فروندی همراه با پرتابه‌های کاذب و جنگ الکترونیک به یک سامانه حمله می‌کنند، کانال‌های درگیری پدافند اشباع شده و سیستم فلج می‌گردد. از سوی دیگر، این استراتژی منجر به فروپاشی روانی اپراتورها در مدیریت بار شناختی (" " Cognitive Load" " Management) می‌شود. در مواجهه با صفحه‌نمایشی که در آن واحد ۵۰۰ هدف با سرعت‌ها و پروفایل‌های پروازی گوناگون را نشان می‌دهد، مغز انسان دچار «فلج تحلیلی» شده و قادر به اولویت‌بندی تهدیدات نخواهد بود. اینجاست که مدافع مجبور می‌شود برای جلوگیری از نفوذ پرتابه‌ها، کنترل پدافند را روی حالت کاملاً خودکار (Auto " " Fire) قرار دهد که خود زمینه را برای فریب الگوریتم‌های پدافندی، تخلیه سریع خشاب‌ها و خطاهای مرگبار شلیک به نیروهای خودی (Friendly " " Fire) فراهم می‌سازد. به این ترتیب، کمیت فناوریانه در دکترین کاوه، پدافند دشمن را از درون متلاشی می‌کند.



فرماندهی جنگ خودمختار

آغاز عصر نبردهای الگوریتمی

بخش چهارم: انسان، عاملیت ماشینی و اخلاق نبرد الگوریتمی

فصل هشتم: طیف سه‌گانه نظارت و مسئله تأخیر مرگبار

(فروپاشی چرخه کلاسیک تصمیم‌گیری و ضرورت خروج انسان از حلقه تاکتیکی)

یکی از بنیادی‌ترین مباحث در دکترین فرماندهی جنگ خودمختار (AutoWarCom)، تعیین جایگاه انسان در معماری نبردهای سایبرنتیک است. در طول تاریخ، ماشین‌ها همواره در امتداد اراده فیزیکی انسان عمل کرده‌اند، اما با ظهور هوش مصنوعی، عاملیت (Agency) به تدریج از اوپراتور انسانی به الگوریتم‌ها منتقل می‌شود. این انتقال عاملیت در یک «طیف سه‌گانه نظارت» تعریف می‌گردد. در سطح نخست، «انسان در حلقه» (Human "-" in "-" the "-" loop) قرار دارد؛ مدلی کلاسیک که در آن ماشین تنها یک ابزار است و تمام تصمیمات حیاتی از جمله شناسایی، رهگیری و شلیک، منوط به فرمان مستقیم انسان است (مانند هدایت پهپادهای پرداتور یا ریپر توسط خلبانان مستقر در پایگاه‌های دوردست). در سطح دوم، «انسان بر حلقه» (Human "-" on "-" the "-" loop) مطرح می‌شود؛ در این معماری، سامانه دارای سطح بالایی از خودمختاری است و می‌تواند اهداف را شناسایی و با آن‌ها درگیر شود، اما انسان به عنوان یک ناظر عالی حضور دارد و دارای یک «دکمه توقف اضطراری» (Veto/Abort) است تا در صورت تشخیص خطای سیستم، فرآیند شلیک را متوقف سازد.

اما نقطه غایی و چالش‌برانگیز دکترین ناصر کاوه، سطح سوم یعنی «انسان بیرون از حلقه» (Human"- " out"- " of"- " the"- " loop) است. در این حالت، انسان تنها قواعد درگیری (Rules of Engagement)، مرزهای جغرافیایی و پارامترهای مأموریت را برای یک سیستم خودمختار یا ازدحام پهبادی (Swarm) تعریف می‌کند و پس از فعال‌سازی، ماشین به‌طور کامل و بدون هیچ‌گونه نیاز به تأیید یا امکان مداخله انسانی، چرخه کشتار را تا انتها مدیریت و اجرا می‌کند.

دلیل اصلی حرکت شتابان ارتش‌های پیشرفته به سوی این سطح از خودمختاری، پدیده‌ای است که در نظریات راهبردی از آن با عنوان «تأخیر مرگبار» (Fatal" " Latency) یاد می‌شود.

در دهه‌های گذشته، سرهنگ جان بوید مفهومی به نام چرخه «اودا» (OODA" " Loop) شامل چهار مرحله «مشاهده، جهت‌گیری، تصمیم‌گیری و اقدام» را معرفی کرد. قانون بنیادین بوید این بود که هر طرفی بتواند چرخه اودای خود را سریع‌تر از دشمن طی کند، پیروز میدان است. در جنگ‌های انسانی، این چرخه در مقیاس دقیقه و ثانیه رخ می‌دهد.

زمان واکنش بیولوژیک انسان برای پردازش یک تصویر بصری حداقل ۲۰۰ تا ۳۰۰ میلی‌ثانیه است و فرآیند شناخت، تحلیل و تصمیم‌گیری به چندین ثانیه زمان نیاز دارد. اما در یک نبرد خودمختار، سامانه‌های مجهز به هوش مصنوعی لبه (Edge AI) محیط را در مقیاس نانو ثانیه و میکروثانیه پردازش می‌کنند. این تفاوت فاحش در معادله زیر تجلی می‌یابد:

$$\Delta t_{\text{Algorithmic}} \ll \Delta t_{\text{(Human " " Cognition)}}$$

هنگامی که یک ناو جنگی با حمله همزمان و هماهنگ ده‌ها موشک هایپر سونیک و ریزپرنده کامیکازه روبه‌رو می‌شود که با سرعت مافوق صوت و الگوهای پروازی غیرقابل پیش‌بینی حرکت می‌کنند، اصرار بر حفظ «انسان در حلقه» به معنای پذیرش شکست قطعی است. در این محیط فشرده از نظر زمانی، ذهن انسان توانایی درک همزمان صدها متغیر فضایی را ندارد و حضور او نه تنها یک مزیت اخلاقی نیست، بلکه به یک گلوگاه (Bottleneck) شناختی و «تأخیر مرگبار» تبدیل می‌شود. دکترین AutoWarCom استدلال می‌کند که در چنین شرایطی، فروپاشی چرخه تصمیم‌گیری انسان اجتناب‌ناپذیر است و فرماندهی باید به شبکه‌های عصبی مصنوعی سپرده شود تا با سرعتی هم‌تراز با تهدید، دفاع یا حمله متقابل را سازماندهی کنند.

«عصر ارتش‌های خودمختار و نبردهای الگوریتمی»

ناصر کاوه با همکاری هوش مصنوعی (Gemini)



فصل نهم: معماری مسئولیت، پاسخ‌گویی و توقف ایمن

(بحران عاملیت حقوقی و گذار از توهم کنترل به ممیزی‌پذیری سامانه‌ها)

با پذیرش ضرورت عملیاتی خروج انسان از حلقه تاکتیکی (Human"- " out"- " of"- " the"- " loop)، دکترین AutoWarCom با مهیب‌ترین چالش حقوقی و اخلاقی تاریخ نبرد مواجه می‌شود: «مسئله انتساب مسئولیت». در حقوق بین‌الملل بشردوستانه (IHL) و کنوانسیون‌های ژنو، مفاهیمی چون تفکیک (میان نظامیان و غیرنظامیان) و تناسب، بر پایه «نیت و قضاوت آگاهانه انسانی» بنا شده‌اند. اگر یک سیستم خودمختار در میدان نبرد دچار خطای محاسباتی شود و یک بیمارستان یا اتوبوس غیرنظامی را به عنوان هدف نظامی شناسایی و منهدم کند، چه کسی به عنوان جنایت‌کار جنگی محاکمه خواهد شد؟

در اینجا با شبکه‌ای درهم‌تنیده از توزیع مسئولیت روبه‌رو هستیم: فرماندهی که دستور استقرار سیستم را داده است؟

مهندس نرم‌افزار و طراح الگوریتم شبکه‌های عصبی (که ممکن است ندانسته سوگیری‌های داده‌ای یا Biases را وارد کد کرده باشد)؟
کارخانه سازنده سنسورها؟

یا نهاد ناظر نظامی؟

این خلأ حقوقی، نیازمند معماری نوینی از مسئولیت‌پذیری است که فراتر از دادگاه‌های کلاسیک نظامی عمل کند.

یکی از نقدهای بنیادین دکترین ناصر کاوه به رویکردهای محافظه‌کارانه (که بر حفظ مدل «انسان بر حلقه» پافشاری می‌کنند)، افشای پدیده «توهم کنترل انسانی» است. طراحان سامانه‌های نیمه‌خودمختار مدعی‌اند که با قرار دادن یک اپراتور انسانی به عنوان ناظر نهایی، الزامات اخلاقی را رعایت کرده‌اند. اما واقعیت شناختی نشان می‌دهد که وقتی یک الگوریتم به‌ظاهر بی‌نقص در میان صدها هدف، یکی را با رنگ قرمز روی مانیتور مشخص می‌کند و به اپراتور تنها ۳ تا ۵ ثانیه زمان برای وتوی شلیک (Veto " " Window) می‌دهد، اپراتور دچار «سوگیری اتوماسیون» (Automation " " Bias) می‌شود.

در این حالت، انسان به دلیل فشار روانی، خستگی و اعتماد مفرط به ماشین، عملاً هیچ بررسی انتقادی روی تصمیم سیستم انجام نداده و صرفاً به عنوان یک «مُهر تأیید لاستیکی» (Rubber Stamp) برای مشروعیت بخشیدن به شلیک عمل می‌کند. این حضور نمایشی انسان، نه تنها اخلاقی نیست، بلکه صرفاً سازوکاری برای فرافکنی مسئولیت از ماشین به سرباز است.

برای حل این بحران، دکترین معماری جنگ خودمختار پیشنهاد می‌دهد که اخلاق باید از مرحله عملیات به مرحله «طراحی الگوریتم» منتقل شود. این امر نیازمند دو رویکرد مهندسی است. نخست، طراحی مسیرهای شکست ایمن (Fail-"- Safe). سیستم‌های خودمختار باید دارای پروتکل‌های غیرقابل نفوذی باشند که اگر ارتباط آن‌ها با شبکه قطع شد، جی‌پی‌اس مختل گردید یا نتوانستند هدف را با ضریب اطمینان بالای

۹۸ درصد تطبیق دهند، به جای حمله کور، به صورت خودکار مأموریت را لغو کرده، در محیطی امن خودتخریبی کنند یا به پایگاه بازگردند. سیستم نباید در حالت اب مسئولیت‌پذیری است که فراتر از دادگاه‌های کلاسیک نظامی عمل کند.

یکی از نقدهای بنیادین دکترین ناصر کاوه به رویکردهای محافظه‌کارانه (که بر حفظ مدل «انسان بر حلقه» پافشاری می‌کنند)، افشای پدیده «توهم کنترل انسانی» است. طراحان سامانه‌های نیمه‌خودمختار مدعی‌اند که با قرار دادن یک اپراتور انسانی به عنوان ناظر نهایی، الزامات اخلاقی را رعایت کرده‌اند.

اما واقعیت شناختی نشان می‌دهد که وقتی یک الگوریتم به‌ظاهر بی‌نقص در میان صدها هدف، یکی را با رنگ قرمز روی مانیتور مشخص می‌کند و به اپراتور تنها ۳ تا ۵ ثانیه زمان برای وتوی شلیک (Veto " " Window) می‌دهد، اپراتور دچار «سوگیری اتوماسیون» (Automation " " Bias) می‌شود. در این حالت، انسان به دلیل فشار روانی، خستگی و اعتماد مفرط به ماشین، عملاً هیچ بررسی انتقادی روی تصمیم سیستم انجام نداده و صرفاً به عنوان یک «مهر تأیید لاستیکی» (Rubber Stamp) برای مشروعیت بخشیدن به شلیک عمل می‌کند. این حضور نمایشی انسان، نه تنها اخلاقی نیست، بلکه صرفاً سازوکاری برای فرافکنی مسئولیت از ماشین به سرباز است. برای حل این بحران، دکترین معماری جنگ خودمختار پیشنهاد می‌دهد که اخلاق باید از مرحله عملیات به مرحله «طراحی الگوریتم» منتقل شود.

این امر نیازمند دو رویکرد مهندسی است. نخست، طراحی مسیرهای شکست ایمن (Fail-" Safe). سیستم‌های خودمختار باید دارای پروتکل‌های غیرقابل نفوذی باشند که اگر ارتباط آن‌ها با شبکه قطع شد، جی‌پی‌اس مختل گردید یا نتوانستند هدف را با ضریب اطمینان بالای ۹۸ درصد تطبیق دهند، به جای حمله کور، به صورت خودکار مأموریت را لغو کرده، در محیطی امن خودتخریبی کنند یا به پایگاه بازگردند. سیستم نباید در حالت ابهام، حالت پیش‌فرض شلیک (Default" " to" " Fire) را انتخاب کند.

دوم و مشاهده روند فکر chevron_left

مهم‌ترین الزام، غلبه بر چالش «جعبه سیاه تصمیم‌گیری» (Black" " Box" " Decision"-" Making) و ایجاد الزام سخت‌گیرانه برای ممیزی‌پذیری کدهای الگوریتمی (Algorithm" " Auditability) است. در مدل‌های پیشرفته یادگیری ماشین، به‌ویژه شبکه‌های عصبی عمیق (Deep" " Neural" " Networks)، فرآیند رسیدن از ورودی‌های خام (مانند تصاویر حرارتی و داده‌های راداری) به خروجی نهایی (تصمیم به شلیک)، درون یک فضای ریاضیاتی پنهان و غیرقابل تفسیر رخ می‌دهد.

به عبارت دیگر، حتی برنامه‌نویسان و سازندگان این سامانه‌ها نیز در بسیاری از مواقع دقیقاً نمی‌دانند سیستم بر اساس چه منطقی هدف الف را به هدف ب ترجیح داده است. پذیرش این تاریکی محاسباتی در میدان نبرد که جان انسان‌ها در میان است، از منظر حقوقی و اخلاقی کاملاً مردود است.

برای حل این بحران، دکترین کاوه بر پیاده‌سازی مفهوم «هوش مصنوعی توضیح‌پذیر» (AI "Explainable" یا XAI) در طراحی تسلیحات خودمختار تأکید دارد. هر سامانه مرگبار الگوریتمی باید به یک سیستم ثبت داده‌های غیرقابل تغییر متصل باشد (چیزی شبیه به جعبه سیاه هواپیما، اما در مقیاس کدهای کامپیوتری و با بهره‌گیری از فناوری‌های رمزنگاری مانند بلاک‌چین‌های خصوصی نظامی).

در این معماری، هر تصمیمی که ماشین در محیط می‌گیرد، همراه با وزن‌های شبکه‌های عصبی، داده‌های سنسوری در آن میلی‌ثانیه خاص و مسیر استنتاج منطقی آن ثبت می‌شود.

در صورت بروز خطای مرگبار (مانند حمله به اهداف غیرنظامی یا نیروهای خودی)، تیم‌های ممیزی مستقل نظامی و حقوقی باید بتوانند با باز کردن این جعبه سیاه دیجیتال، فرآیند را مهندسی معکوس کنند. آن‌ها باید دقیقاً مشخص کنند که خطا از کجا ناشی شده است: آیا سنسور سخت‌افزاری دچار اختلال شده و داده آلوده (Poisoned "Data") دریافت کرده است؟

آیا پایگاه داده آموزشی (Training "Dataset") در آزمایشگاه دارای سوگیری بوده است؟ یا اینکه فرمانده میدان، سیستم را خارج از پارامترهای عملیاتی تأییدشده (مثلاً در یک محیط متراکم شهری به جای دشت باز) مستقر کرده است؟

با این معماری نوین پاسخ‌گویی، توزیع مسئولیت شفاف می‌گردد. مفهوم «پاسخ‌گویی» از لحظه و مکان فشردن ماشه (که در جنگ‌های کلاسیک رخ می‌داد)، به آزمایشگاه‌های نرم‌افزاری، پایگاه‌های داده و مراحل تأیید صلاحیت (Certification) در کارخانه‌های تسلیحاتی منتقل می‌شود.

در این دکترین، فرمانده نظامی در صورتی که سیستم را مطابق پروتکل‌های استاندارد فعال کرده باشد از اتهام جنایت جنگی مبرا است و زنجیره پاسخ‌گویی مستقیماً گریبان نهاد توسعه‌دهنده، طراحان الگوریتم و تأییدکنندگان معماری Fail-Safe را می‌گیرد.

نتیجه‌گیری بخش چهارم:

دکترین «فرماندهی جنگ خودمختار» (AutoWarCom) با عبور از رمانتیسم حفظ نمایشی انسان در حلقه، واقعیت مهیب جنگ‌های فرکانس‌بالا و سرعت پردازش الگوریتمی ($\Delta t_{\text{Human}} \ll \Delta t_{\text{Algorithmic}}$) را می‌پذیرد.

با این حال، تسلیم جبر ماشین نمی‌شود، بلکه با انتقال مرزهای اخلاق و کنترل از «میدان نبرد» به «مرحله طراحی و معماری نرم‌افزار»، تضمین می‌کند که حتی در غیاب کامل انسان از حلقه تاکتیکی، ماشین‌ها دقیقاً در چارچوب اراده راهبردی، حقوق بشردوستانه و پروتکل‌های سخت‌گیرانه ممیزی‌پذیر عمل کنند. این تکامل، ضامن بقای نیروی نظامی در برابر هر جومرج نهفته در نبردهای خودمختار خواهد بود.

فرماندهی جنگ خودمختار

آغاز عصر نبردهای الگوریتمی



ناصر کاوه

بخش پنجم: کالبدشکافی ترورهای هدفمند؛ تکامل ۸۰ ساله و چهار بازوی نوین

فصل دهم: گاه‌شمار ۸۰ ساله ترور در دکترین امنیتی اسرائیل (۱۹۴۸ تا کنون)

(از نفوذ فیزیکی تا ماشین ترور داده‌محور)

دکترین امنیتی و نظامی رژیم صهیونیستی از بدو تأسیس تاکنون، وابستگی عمیق و ساختاری به استراتژی «ترورهای هدفمند» (Targeted Assassinations) داشته است. این استراتژی در طول هشت دهه گذشته، همگام با تحولات تکنولوژیک جهانی، چهار عصر متمایز را پشت سر گذاشته است که بررسی آن برای درک معماری جنگ خودمختار امری حیاتی است.

عصر اول (۱۹۴۸-۱۹۸۰): نفوذ فیزیکی و جاسوسی انسانی (HUMINT)

در دهه‌های نخست، معماری ترور کاملاً بر پایه منابع انسانی استوار بود. در این دوره، شناسایی، تعقیب و حذف فیزیکی اهداف نیازمند ماه‌ها یا سال‌ها کار اطلاعاتی توسط شبکه‌های نفوذی و جاسوسان میدانی بود. بخش ویژه «کیدون» در موساد با استفاده از جوخه‌های ترور کماندویی، بمب‌گذاری‌های دستی و عملیات‌های فیزیکی در کشورهای هدف اقدام می‌کرد.

این روش اگرچه در آن زمان مؤثر می‌نمود، اما به شدت زمان‌بر، پرهزینه و دارای ریسک بالای لو رفتن شبکه‌های انسانی بود.

عصر دوم (۱۹۸۰-۲۰۰۰): تلفیق رهگیری مخابراتی (SIGINT) و اپتیک هوایی (IMINT)

با پیشرفت فناوری‌های ارتباطی، دکترین ترور وارد فاز ترکیبی شد. در این عصر، شنود مکالمات رادیویی و تلفنی (SIGINT) با نظارت هوایی توسط پهپادهای اولیه و هواپیماهای شناسایی (IMINT) ادغام گردید. برجسته‌ترین نماد این دوره، استفاده از بالگردها و جنگنده‌ها برای شلیک موشک‌های هدایت‌شونده به سمت خودروی رهبران مقاومت (نظیر ترور شهید سید عباس موسوی و شهید فتحی شقاقی) بود. در این مرحله، اگرچه سرعت واکنش افزایش یافت، اما همچنان نیازمند تأیید نهایی و خطایابی توسط یک زنجیره انسانی طولانی بود.

عصر سوم (۲۰۰۰-۲۰۲۰): انباشت کلان‌داده‌ها و نفوذ سایبری زیرساختی

با ظهور اینترنت و گوشی‌های هوشمند، واحد ۸۲۰۰ ارتش اسرائیل معماری اطلاعاتی خود را به سمت «شنود انبوه و جمع‌آوری متاداده‌ها» تغییر داد. در این دوره، بدافزارهای تجسسی بدون نیاز به کلیک قربانی (Zero-"Click" Spyware) و معماری‌های پیچیده‌ای نظیر نرم‌افزار پگاسوس (Pegasus) توسعه یافتند. این سیستم‌ها با نفوذ به لایه‌های پنهان سیستم عامل، میکروفون، دوربین و پیام‌های رمزنگاری‌شده را به یک ابزار جاسوسی بلادرنگ تبدیل کردند.

هدف در این عصر، صرفاً شنود یک فرد نبود، بلکه استخراج تمام الگوهای زیستی و ارتباطی جامعه هدف بود.

عصر چهارم (۲۰۲۰ به بعد): گذار به ماشین ترور داده‌محور و یادگیری عمیق

چالش اصلی در پایان عصر سوم، انفجار اطلاعات بود. حجم کلان‌داده‌های جمع‌آوری شده از شبکه‌های اجتماعی، دوربین‌های مداربسته، متاداده‌های ارتباطی و حسگرهای محیطی به قدری عظیم شد که هزاران تحلیل‌گر انسانی نیز قادر به پردازش آن‌ها نبودند. در اینجا بود که دکترین نظامی اسرائیل وارد فاز چهارم شد:

واگذاری کامل فرآیند استخراج هدف به الگوریتم‌های هوش مصنوعی و یادگیری عمیق (Deep " " Learning).

در این عصر، انسان از چرخه تولید هدف خارج شده و ماشین به تنهایی تصمیم می‌گیرد چه کسی، در چه زمانی و با چه توجیهی باید از میان برداشته شود.

این تحول، بستر اصلی شکل‌گیری «چهار بازوی نوین ترور الگوریتمی» را فراهم آورد که کالبدشکافی آن‌ها در فصل بعد مورد بررسی قرار می‌گیرد.



AI COMMAND & CONTROL

- ANALYZE
- DECIDE
- EXECUTE
- AUTONOMOUS

DRONE SWARM



- AIR
- LAND
- SEA
- SPACE
- CYBER

فرماندهی جنگ خودمختار

آغاز عصر نبردهای الگوریتمی

ناصر کاوه

فصل یازدهم: بازوهای چهارگانه ترورهای الگوریتمی مدرن

(معماری مرگ در عصر ماشین‌های هوشمند)

در دکترین مدرن فرماندهی جنگ خودمختار (AutoWarCom)، عملیات ترور از یک اقدام نقطه‌ای و انسانی به یک «خط تولید صنعتی و کاملاً الگوریتمی» تبدیل شده است. این خط تولید بر چهار بازوی درهم‌تنیده استوار است که به‌طور یکپارچه عمل کرده و چرخه OODA را در کسری از ثانیه تکمیل می‌کنند. بازوی اول: هوش مصنوعی و اتوماسیون کارخانه تولید هدف هسته مرکزی این بازو، واگذاری فرآیند کشف هدف به ماشین است. سامانه‌ای نظیر هَبسورا (Habsora یا گاسپل)، با استفاده از بینایی ماشین و پردازش بلادرنگ تصاویر ماهواره‌ای و رادارهای سار (SAR)، تغییرات ساختمانی و پایگاه‌های فیزیکی را شناسایی می‌کند. اما بعد انسانی ماجرا به سامانه مخوف‌تری به نام لاوندر (Lavender) سپرده شده است. لاوندر با تحلیل متاداده‌های ارتباطی و نظارت بر گروه‌های پیام‌رسان (نظیر واتس‌آپ)، به صدها هزار فرد امتیازی بین ۱ تا ۱۰۰ می‌دهد و افراد با امتیاز بالا را به عنوان «هدف ترور» علامت‌گذاری می‌کند. سامانه‌های مکمل نظیر «کجاست بابا؟» (Where's "Daddy"?) و «کیمیایگر» (Alchemist) نیز با استفاده از سنسورها، لحظه دقیق ورود فرد به خانه را برای شلیک نهایی به شبکه اعلام می‌کنند. در این بازو، توجیه تلفات غیرنظامیان توسط فرمول‌های اداری-محاسباتی مانند نازا (NAZA) صورت می‌گیرد که به‌طور سیستماتیک، مرگ ده‌ها زن و کودک را برای حذف یک هدف سطح پایین، «مشروع و مجاز» جلوه می‌دهد.

بازوی دوم: پردازش گراف جامعه و مدل‌سازی ریاضی روابط (Social " " Graph " " Analytics) ماشین‌های ترور نوین، افراد را به صورت ایزوله نمی‌بینند، بلکه آن‌ها را در قالب شبکه‌های ریاضی مدل‌سازی می‌کنند. در این معماری، جامعه هدف به عنوان یک گراف $G=(V \textcircled{m}, E)$ تعریف می‌شود که در آن، افراد، سیم‌کارت‌ها و دستگاه‌ها به مثابه گره (Node) و تماس‌ها یا حضورهای فیزیکی مشترک به عنوان یال (Edge) در نظر گرفته می‌شوند. الگوریتم‌ها با محاسبه مرکزیت بینابینی ("Betweenness Centrality") و مرکزیت بردار ویژه (Eigenvector " " Centrality)، نه تنها فرماندهان پنهان، بلکه واسطه‌ها، رانندگان و اعضای خانواده را شناسایی می‌کنند. از طریق خوشه‌بندی رفتار اطرافیان، گراف ساده ارتباطات به یک «گراف ترور» تبدیل می‌شود که در آن، نقطه ضعف یک رهبر نه در فناوری شخصی او، بلکه در رفتار دیجیتال اطرافیانش نهفته است.

بازوی سوم: استنتاج موقعیت بدون جی‌پی‌اس و آلوده‌سازی زنجیره تأمین هنگامی که اهداف از حمل تجهیزات جی‌پی‌اس‌دار خودداری می‌کنند، الگوریتم‌ها از روش‌های استنتاجی استفاده می‌نمایند. تکنیک‌هایی نظیر اثر انگشت امواج بی‌سیم (Wi-"- Fi" " Fingerprinting)، پیش‌روی زمانی دکل‌های مخابراتی (Timing" " Advance) و همجوشی حسگرها (Sensor" " Fusion) موقعیت دقیق فرد را بدون نیاز به ماهواره استخراج می‌کنند. اما بُعد پیچیده‌تر این بازو، سلاح‌سازی اقلام روزمره از طریق نفوذ به زنجیره تأمین جهانی است. همان‌طور که در رویداد سپتامبر ۲۰۲۴ در لبنان مشاهده شد، سازمان‌های اطلاعاتی

با ایجاد شرکت‌های پوششی اروپایی و نفوذ عمیق به خطوط تولید، مواد منفجره پر قدرت نظیر PETN و چاشنی‌های مینیاتوری را در پیجرها و بی‌سیم‌های سازمانی تعبیه کردند. این روش، مرز میان تجهیزات غیرنظامی و بمب‌های ساعتی را به‌طور کامل از بین می‌برد.

بازوی چهارم: سکوهای تسلیحاتی خودمختار ضارب نهایی (Kinetic " " Platforms) بازوی نهایی در این معماری، مجریان فیزیکی ترور هستند. این سکوها نیازی به خلبان یا تکتیرانداز ندارند.

تیربارهای رباتیک هدایت‌شونده از طریق ماهواره که مجهز به هوش مصنوعی و پردازش تصویر برای شناسایی چهره هستند (نظیر آنچه در ترور شهید محسن فخری‌زاده در آذر ۱۳۹۹ استفاده شد)، مهمات پرسه‌زن انتحاری (Loitering " " Munitions) و کوادکوپترهای خودمختاری که در محیط‌های متراکم شهری بدون نیاز به هدایت اپراتور اهداف را تعقیب و منهدم می‌کنند، اضلاع نهایی این ساختار را تشکیل می‌دهند.

این ماشین‌ها، چرخه کشتار را با دقتی بی‌رحمانه و سرعتی فراتر از واکنش انسانی به پایان می‌رسانند.

AUTONOMOUS WARFARE COMMAND

AUTOWARCOM

SENSOR → DECISION → SHOOTER

PROJECT AGINCOURT

INTEGRATED AUTONOMOUS OPERATIONS

- AI COMMAND & CONTROL
- MULTI-DOMAIN AUTONOMY
- KILL WEB NETWORK
- REAL-TIME ADAPTATION



KILL WEB

CONNECTED · DISTRIBUTED · LETHAL



- GLOBAL SENSORS
- AI ANALYTICS
- AUTONOMOUS DECISIONS
- PRECISION STRIKE

فرماندهی جنگ خودمختار

AIR DOMAIN

- SWARM DRONES
- UCAVS
- ISR PLATFORMS

LAND DOMAIN

- UGVs
- ROBOTIC PLATFORMS
- AUTONOMOUS LOGISTICS

SEA DOMAIN

- AUTONOMOUS SUBMARINES
- USVs
- MINE COUNTERMEASURES



STATE OF THE FORCE



PLATFORMS
247



AUTONOMY
LEVEL
HIGH



GLOBAL
COVERAGE
92%



THREAT
RESPONSE
< 5s

ناصرکاوه

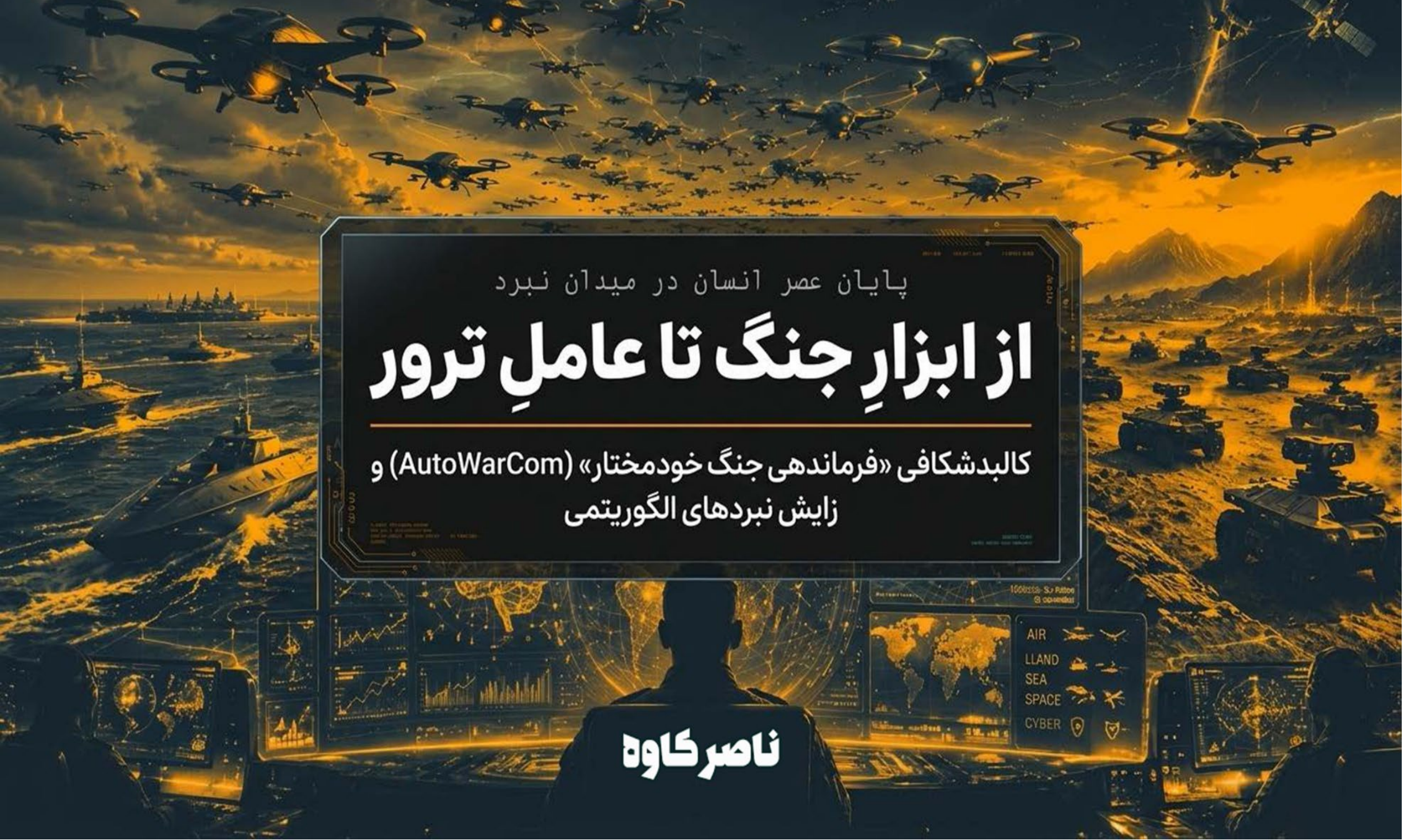
فصل دوازدهم: تمایز دستاورد تاکتیکی از پیروزی استراتژیک

(بحران دکترین رهبری‌زدایی در برابر ساختارهای عقیدتی)

اگرچه معماری ترورهای الگوریتمی و بازوهای چهارگانه آن دستاوردهای تاکتیکی خیره‌کننده‌ای برای ماشین جنگی غرب و رژیم صهیونیستی به همراه داشته است، اما دکترین ناصر کاوه (AutoWarCom) بر یک تمایز بنیادین تأکید دارد: «موفقیت تاکتیکی هرگز تضمین‌کننده پیروزی استراتژیک نیست». اتکای افراطی به ترور فرماندهان بر پایه یک فرض غلط بنا شده است و آن اثربخشی «دکترین رهبری‌زدایی» (Decapitation " " Strategy) است. دکترین رهبری‌زدایی فرض می‌کند که سازمان‌های نظامی-سیاسی، ساختارهایی هرمی و قائم‌به‌شخص هستند که با قطع کردن رأس هرم (فرماندهان ارشد)، کل سازمان دچار فروپاشی، سردرگمی و فلج عملیاتی می‌شود. این تئوری شاید در مورد ارتش‌های کلاسیک یا گروه‌های مافیایی صدق کند، اما در مواجهه با ساختارهای عقیدتی و منعطف محور مقاومت با شکستی فاحش روبه‌رو شده است. سازمان‌هایی نظیر حزب‌الله لبنان، حماس و دیگر اجزای محور مقاومت، دارای معماری شبکه‌ای، سلولی و مبتنی بر ایدئولوژی هستند، نه صرفاً کاریزمای شخصی.

در این ساختارهای عقیدتی، شهادت یک فرمانده ارشد نه تنها موجب فروپاشی نمی‌شود، بلکه به عنوان یک «کاتالیزور انگیزشی» و عنصر تقویت‌کننده انسجام سازمانی عمل می‌کند. سیستم‌های جانشین‌پروری منعطف باعث می‌شوند که کادرهای فرماندهی در سطوح میانی، به سرعت و در عرض چند روز یا چند ساعت، جای خالی رهبران پیشین را پر کنند. این بازسازی سریع، نشان‌دهنده «تاب‌آوری ارگانیسم» در برابر حملات سایبرنتیک و الگوریتمی است.

علاوه بر این، تمرکز بیش از حد بر ترورهای فناوری‌محور، منجر به غفلت از دینامیک‌های کلان‌بازدارندگی متقابل شده است. هنگامی که یک طرف با استفاده از هوش مصنوعی خطوط قرمز را جابه‌جا کرده و دست به ترورهای گسترده می‌زند، طرف مقابل نیز با بهره‌گیری از اصل غافلگیری، جنگ نامتقارن، اشباع پدافندی (از طریق ازدحام موشکی و پهپادی) و ضربات فلج‌کننده به زیرساخت‌های اقتصادی و جمعیتی، چرخه‌های جدیدی از بازدارندگی را تحمیل می‌کند. در نهایت، پیشرفته‌ترین الگوریتم‌های هوش مصنوعی (نظیر لاوندِر) و مرگبارترین زنجیره‌های ترور، ممکن است در کوتاه مدت ضربات دردناکی وارد کنند، اما در بلندمدت قادر به تغییر اراده سیاسی، ریشه‌کن کردن پایگاه اجتماعی و غلبه بر اراده استراتژیک یک ملت سازمان‌یافته و عقیدتی نخواهند بود. پدیده جنگ خودمختار، اگرچه فرم نبرد را تغییر داده، اما ماهیت پیروزی را همچنان در گرو اراده انسانی باقی گذاشته است.



پایان عصر انسان در میدان نبرد

از ابزار جنگ تا عامل ترور

کالبدشکافی «فرماندهی جنگ خودمختار» (AutoWarCom) و
زایش نبردهای الگوریتمی

ناصر کاوه

بخش ششم: سناریوهای تهدید نامتقارن، تسلیحات غیردولتی و پیامدهای امنیتی

فصل سیزدهم: دموکراتیزه شدن تسلیحات خودمختار و بازیگران غیردولتی

(پایان انحصار دولت‌ها بر خشونت نقطه‌زن)

یکی از مهم‌ترین پیامدهای دکنترین جنگ خودمختار، پدیده‌ای است که استراتژیست‌ها از آن با عنوان «دموکراتیزه شدن تسلیحات مرگبار» یاد می‌کنند. در قرن بیستم و اوایل قرن بیست‌ویکم، توسعه سلاح‌های نقطه‌زن و پهپادهای شناسایی-رزمی (مانند پرداتور یا ریپر) نیازمند بودجه‌های میلیارد دلاری، زیرساخت‌های عظیم ماهواره‌ای و صنایع پیشرفته هوافضا بود. این انحصار تکنولوژیک باعث می‌شد که قدرت اعمال خشونت دقیق، منحصرأ در اختیار دولت‌های بزرگ و ارتش‌های کلاسیک باقی بماند.

اما امروز، همگرایی دو موج فناوری یعنی سخت‌افزارهای تجاری ارزان‌قیمت (COTS) و کدهای هوش مصنوعی متن‌باز ("Open" AI " Source)، این انحصار تاریخی را در هم شکسته و بازیگران غیردولتی، گروه‌های شبه‌نظامی و حتی هسته‌های کوچک مقاومت را به توانمندی‌های راهبردی مجهز کرده است.

فرآیند این دموکراتیزه شدن به این شکل عمل می‌کند: یک کوادکوپتر تجاری ساده (مانند محصولات DJI یا پهپادهای مسابقه‌ای FPV) که با قیمتی کمتر از ۵۰۰ دلار در بازار آزاد قابل تهیه است، با نصب یک برد پردازشی کوچک (نظیر Raspberry Pi یا Jetson Nano) و بارگذاری الگوریتم‌های رایگان و متن‌باز در حوزه بینایی ماشین (مانند نسخه‌های مختلف YOLO برای تشخیص اشیاء و چهره)، به یک سلاح خودمختار مخوف تبدیل می‌شود.

در گذشته، اجرای یک عملیات ترور هدفمند یا انهدام یک فرمانده در میدان نبرد، نیازمند سال‌ها آموزش برای تربیت یک تکتیرانداز ماهر بود تا بتواند متغیرهایی نظیر سرعت باد، افت گلوله، رطوبت و تنفس خود را محاسبه کند.

امروز، یک نوجوان با دانش متوسط برنامه‌نویسی می‌تواند با استفاده از کدهای AI "Open"-Source، پرنده‌ای بسازد که تنها با دریافت یک عکس از هدف، او را در میان جمعیت تشخیص داده و با سرعت بالا به سمت وی هجوم ببرد.

این تغییر پارادایم، مهارت فیزیکی را با «کدنویسی الگوریتمی» جایگزین کرده است.

با این حال، این تسلیحات ارزان‌قیمت و دست‌ساز، چالش‌های امنیتی و عملیاتی بی‌سابقه‌ای را به همراه دارند که مهم‌ترین آن‌ها، مسئله قطع ارتباط و از دست رفتن کنترل پرواز است.

از آنجا که این پهپادها برای فرار از پارازیت‌ها و سامانه‌های جنگ الکترونیک (EW) دشمن طراحی می‌شوند، پس از قفل شدن روی هدف و آغاز حمله، ارتباط رادیویی خود را با اپراتور قطع می‌کنند تا قابل ردیابی نباشند. این پروتکل که به عنوان شلیک و فراموش ("Fire"- "Forget" and) شناخته می‌شود، سیستم را در حالت خودمختاری کامل قرار می‌دهد. اما فقدان پیوند ماهواره‌ای یا رادیویی به این معناست که اپراتور هیچ راهی برای «لغو مأموریت» (Abort Mission) ندارد.

اگر پس از شلیک پرتابه، هدف وارد یک محیط پرتراکم غیرنظامی (مانند یک بازار یا مدرسه) شود، یا اگر هوش مصنوعی پردازشگر لبه (AI "Edge") دچار خطای محاسباتی شده و فرد دیگری را که شباهت ظاهری به هدف دارد انتخاب کند، انسان فرستنده هیچ مکانیزمی برای متوقف کردن فاجعه نخواهد داشت. ماشین بر اساس منطق کامپایل شده خود تا لحظه انفجار پیش می‌رود. این استقلال مطلق، اگرچه در برابر سامانه‌های پدافندی و اخلاص‌گرها یک مزیت تاکتیکی بی‌نظیر برای گروه‌های نامتقارن محسوب می‌شود، اما در عین حال مرزهای اخلاقی و تفکیک میان نظامیان و غیرنظامیان را به شدت مخدوش کرده و کنترل پیامدهای نبرد را از دست انسان خارج می‌سازد.



زایش فرماندهی جنگ خودمختار (AutoWarCom)

وقتی ماشین از ابزارِ نبرد، به عاملِ مرگ و ترور تبدیل می‌شود.

گذر از عصر سلاح‌های تحت فرمان انسان، به عصر
عصر نبردهای الگوریتمی و عاملیت ماشین.

اعلامیه رسمی: تأسیس فرماندهی یکپارچه رزمی ۴
ستاره برای تسریع و تجمیع سامانه‌های خودمختار.

فصل چهاردهم: پیامدهای راهبردی ترورهای خودمختار برای بازیگران دولتی

(ابهام در انتساب، خطای الگوریتمی و تصاعد ناخواسته بحران)

استفاده از تسلیحات خودمختار و الگوریتم‌های ترور، نه تنها برای گروه‌های غیردولتی، بلکه برای بازیگران دولتی نیز پیامدهای راهبردی عمیقی به دنبال داشته است. در نگاه اول، ارتش‌های مدرن و سرویس‌های اطلاعاتی (به ویژه دولت‌های غربی و رژیم صهیونیستی) به این تسلیحات به چشم ابزارهایی برای اعمال «دقت جراحی» (Surgical Precision) می‌نگرند؛ ابزارهایی که می‌توانند بدون به خطر انداختن جان نیروهای خودی، اهداف کلیدی را در عمق خاک دشمن نابود کنند. اما این رویکرد، در سطح کلان منجر به «عادی‌سازی نقض حاکمیت ملی» کشورها شده است.

هنگامی که یک دولت می‌تواند با ارسال یک ریزپرنده خودمختار، هدفی را در پایتخت کشوری دیگر ترور کند و به دلیل ابعاد کوچک سلاح، سامانه‌های راداری کلاسیک قادر به کشف آن نیستند، مفهوم حریم هوایی و مرزهای جغرافیایی عملاً فرو می‌ریزد. این عادی‌سازی تجاوز، آستانه تحمل و خطوط قرمز سنتی در روابط بین‌الملل را تغییر داده و وضعیت دائمی «جنگ در منطقه خاکستری» را تثبیت می‌کند.

یکی از خطرناک‌ترین ویژگی‌های راهبردی این تسلیحات، ایجاد پوشش محافظتی «انکارپذیری موجه» (Plausible " " Deniability) برای دولت‌های مهاجم است. در ترورهای سنتی با جنگنده‌ها یا موشک‌های کروز، رهگیری مسیر پرتاب و بررسی قطعات به‌جای‌مانده (که دارای شماره سریال و هویت کارخانه‌ای بودند)، به وضوح کشور مهاجم را مشخص می‌کرد.

اما در عصر جنگ خودمختار، یک دولت می‌تواند کدهای ترور را روی پهپادهایی پیاده‌سازی کند که قطعات آن‌ها از بازارهای تجاری کشورهای مختلف خریداری شده و با چاپگرهای سه‌بعدی مونتاژ شده‌اند. این سلاح‌های بدون هویت و فاقد مسیر پروازی راداری، این امکان را به دولت مهاجم می‌دهند که پس از انجام یک ترور استراتژیک، با قاطعیت هرگونه دخالت را انکار کند. این ابهام در انتساب حمله، مانع از شکل‌گیری یک پاسخ مشروع بین‌المللی شده و ساختارهای حقوقی سازمان ملل را در تشخیص متجاوز فلج می‌سازد.

با این وجود، بزرگ‌ترین تهدید راهبردی که حتی خود دولت‌های بهره‌بردار از این تکنولوژی را نیز به وحشت می‌اندازد، پدیده «خطای طبقه‌بندی مثبت کاذب» (False " " Positive) و خطر تصاعد ناخواسته بحران است. الگوریتم‌های یادگیری ماشین، هرگز بر مبنای قطعیت ۱۰۰ درصدی عمل نمی‌کنند، بلکه تصمیمات آن‌ها بر پایه احتمالات آماری و توابع توزیع ریاضی استوار است.

اگر یک سیستم خودمختار دچار خطای "Positive " False شود (یعنی فرد یا موجودیتی بی‌گناه را به اشتباه به عنوان یک هدف مشروع نظامی طبقه‌بندی کرده و منهدم کند)، عواقب آن در سطح ژئوپلیتیک می‌تواند فاجعه‌بار باشد. تصور کنید یک سامانه خودمختار گشت‌زنی در یک مرز پرتنش، کاروان خودروهای دیپلماتیک یک کشور ثالث یا فرماندهان ارشد یک قدرت هسته‌ای را به دلیل شباهت الگوهای حرکتی، به عنوان یک واحد تروریستی شناسایی کرده و مورد هجوم قرار دهد. در جنگ‌های کلاسیک، در صورت بروز چنین اشتباهی، تلفن‌های سرخ میان سران کشورها به کار می‌افتاد تا با دیپلماسی، مانع از گسترش جنگ شوند؛ زیرا هر دو طرف می‌دانستند که «خطای انسانی» رخ داده است.

اما هنگامی که یک ماشین بدون هیچ‌گونه هشدار قبلی و با بی‌رحمی الگوریتمی دست به ترور می‌زند، کشور آسیب‌دیده این اقدام را نه یک خطای سیستمی، بلکه یک «حمله پیش‌دستانه و استراتژیک» تلقی می‌کند. در این نقطه، خطای یک کد چند خطی پتانسیل آن را دارد که جرقه یک «تصاعد ناخواسته» (Unintended " Escalation) را روشن کرده و یک تنش مرزی مدیریت‌شده را در کسری از ساعت به یک جنگ تمام‌عیار منطقه‌ای یا جهانی تبدیل کند. این پارادوکس، نشان می‌دهد که کنترل تاکتیکی مطلق بر ماشین، به معنای از دست رفتن کنترل استراتژیک بر معماری جنگ است.



ناصر کاوه

ناصر کاوه

فرماندهی جنگ خودمختار

آغاز عصر نبردهای الگوریتمی

بخش هفتم: دکترین جامع پدافند؛ ایجاد کوری اطلاعاتی و تاب‌آوری چندلایه

فصل پانزدهم: پدافند علیه بینایی ماشین و حسگرهای خودمختار

(مهندسی کوری اطلاعاتی؛ از اختلال در ناوبری تا فریب الگوریتم‌ها)

در معماری جنگ خودمختار، برتری دشمن متکی به جریان پیوسته و بی‌نقص داده‌های ورودی از حسگرهای محیطی است. دکترین ناصر کاوه برای خنثی‌سازی این برتری، استراتژی «ایجاد کوری اطلاعاتی» (Information "Blindness") را پیشنهاد می‌دهد. این استراتژی به جای تمرکز انحصاری بر انهدام فیزیکی پلتفرم‌های دشمن (که در برابر ازدحام پهبادی بسیار پرهزینه است)، بر فلج کردن سیستم‌های ادراکی ماشین در سه لایه کلیدی تمرکز دارد: لایه ناوبری، لایه سنسوری و لایه الگوریتمی.

لایه ناوبری: اختلال در SLAM "Visual" و TERCOM

در محیط‌های فاقد جی‌پی‌اس (GPS-"Denied")، پهبادها و موشک‌های خودمختار برای ناوبری به تکنیک‌های تطبیق عوارض زمین (TERCOM) و نقشه‌برداری و موقعیت‌یابی همزمان بصری (SLAM "Visual") متکی هستند. این سیستم‌ها با استخراج نقاط کلیدی از

محیط و مقایسه آن‌ها با نقشه مرجع، مسیر خود را پیدا می‌کنند. پدافند نوین در این لایه، از طریق تزریق ذرات آئروسول (مهدودهای مصنوعی با قابلیت جذب طول‌موج‌های خاص راداری و فروسرخ) در محیط نبرد، میدان دید سنسورها را مختل می‌کند. علاوه بر این، تغییر عամدانه و متناوب هندسه عوارض محیطی (مانند استفاده از سازه‌های کاذب، تورهای استتار هندسی و بازتابنده‌های گوشه‌ای) باعث می‌شود تا ماتریس محاسباتی الگوریتم SLAM دچار واگرایی شده و ماشین در تشخیص موقعیت خود در فضای سه‌بعدی ناتوان بماند.

لایه سنسوری: اشباع اپتیکی و لیزرهای کورکننده

حسگرهای تصویری پهبادهای، بر پایه تراشه‌های CMOS و CCD عمل می‌کنند که به شدت در برابر فوتون‌های متمرکز حساس هستند. در لایه سنسوری، استفاده از لیزرهای کورکننده (Dazzling " " Laser) به عنوان یک ابزار پدافندی نرم مطرح است. تابش پرتوهای لیزر با توان متوسط به سمت عدسی دوربین پهباد مهاجم، باعث اشباع شدن پیکسل‌های سنسور و ایجاد پدیده «شکوفایی» (Blooming) یا کوری موقت دوربین می‌شود. همچنین، استفاده از سیستم‌های ساطع‌کننده سیگنال‌های نوری پالسی با فرکانس‌های نامنظم، الگوریتم‌های تنظیم خودکار نوردهی (Auto-"-" Exposure) و نرخ فریم دوربین را دچار اختلال شدید کرده و خروجی تصویر را به یک صفحه سفید یا پرش‌دار غیرقابل پردازش برای هوش مصنوعی تبدیل می‌کند.

لایه الگوریتمی: پچ‌های تقابلی و مواد تغییر فاز دهنده (PCM)

پیشرفته‌ترین لایه پدافندی، حمله مستقیم به شبکه‌های عصبی پیچشی (CNN) است که مغز متفکر بینایی ماشین را تشکیل می‌دهند.

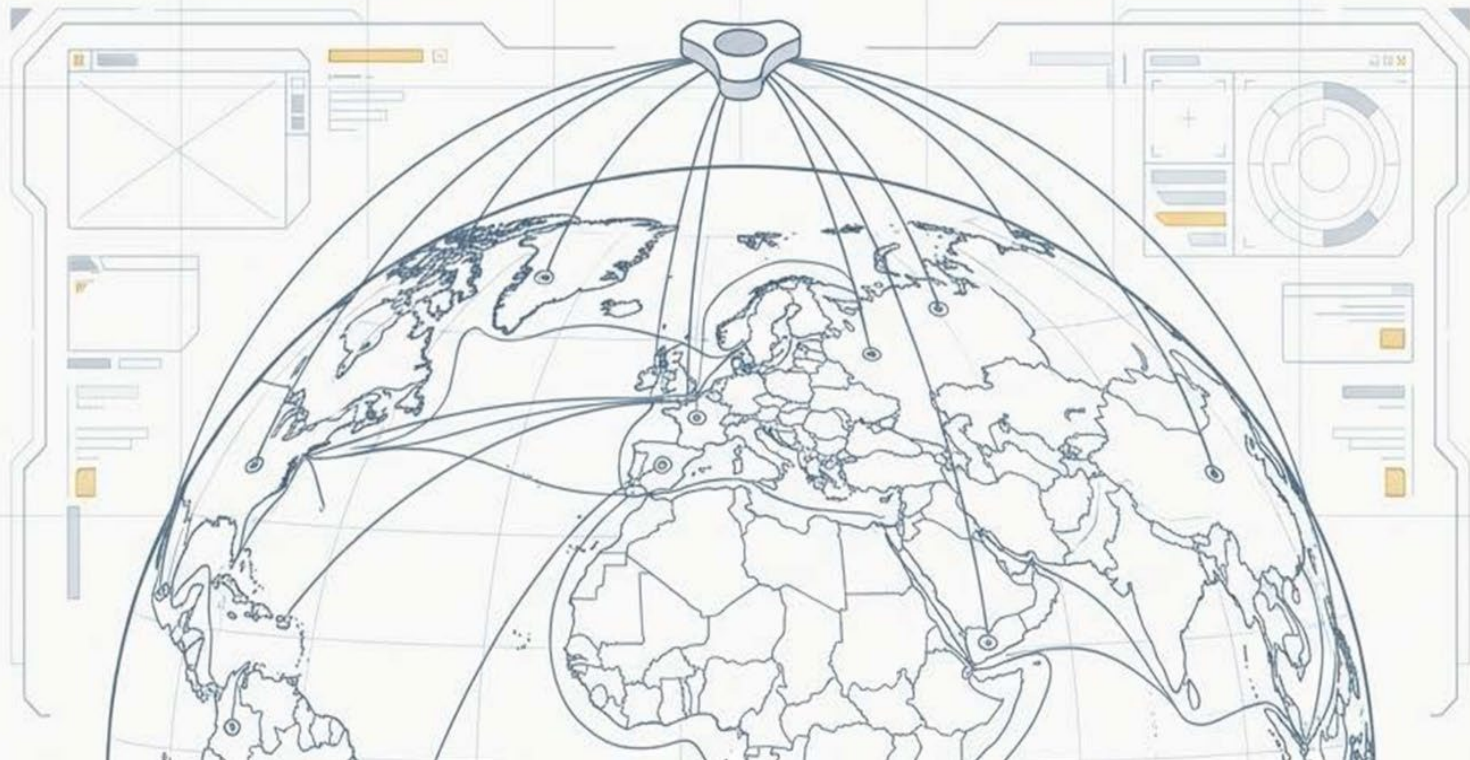
در این راستا، توسعه «پچ‌های تقابلی» (Adversarial " " Patches) – برچسب‌ها یا الگوهای بصری نامنظمی که روی تجهیزات یا یونیفرم‌ها چاپ می‌شوند – باعث می‌شود الگوریتم‌های تشخیص شیء (نظیر YOLO) دچار خطای فاحش شوند؛ به گونه‌ای که یک تانک را به عنوان یک صخره یا یک انسان را به عنوان یک درخت دسته‌بندی کنند.

برای فرار از دید حرارتی و رادارهای لیزری (LIDAR) نیز، استفاده از رنگ‌های نانوساختار جاذب نور (با قابلیت جذب ۹۹ درصد فوتون‌ها) و «مواد تغییر فاز دهنده» (Phase " " Change " " Materials) در دستور کار قرار می‌گیرد.

این مواد، حرارت ساطع‌شده از بدن یا موتور تجهیزات را جذب کرده و آن را هم‌دما با محیط ساطع می‌کنند، که نتیجه آن، پاک شدن کامل امضای حرارتی از دید ترمال‌ویژن‌های دشمن است.

عصر ارتش‌های خودمختار و نبردهای الگوریتمی

کالبدشکافی دکترین فرماندهی ناصر کاوه (AutoWarCom)



فصل شانزدهم: مصون‌سازی زنجیره تأمین سخت‌افزار و پدافند شبکه‌ای

(از آناتومی سخت‌افزاری تا ایزولاسیون گراف‌های ارتباطی)

تجربه حملات سایبرنتیک-فیزیکی اخیر (به‌ویژه رویداد انفجار پیجرها و بی‌سیم‌ها در لبنان) ثابت کرد که در عصر جنگ خودمختار، آسیب‌پذیری تنها به میدان نبرد محدود نمی‌شود، بلکه از خطوط تولید و زنجیره تأمین جهانی آغاز می‌گردد.

دشمن با استفاده از شرکت‌های پوششی، میکروچاشنی‌ها و مدارهای جاسوسی را در معماری داخلی سخت‌افزارهای تجاری پنهان می‌کند. برای مقابله با این استراتژی، دکترین پدافندی نیازمند استقرار سیستم‌های ممیزی بی‌رحمانه و دگرگونی در معماری شبکه‌های سازمانی است.

پروتکل‌های تصویربرداری لایه‌ای و توموگرافی صنعتی

اسکنرهای اشعه ایکس رایج در فرودگاه‌ها و مبادی ورودی، دیگر برای کشف تهدیدات پنهان‌شده در لایه‌های سیلیکونی کافی نیستند. پدافند سخت‌افزاری نوین نیازمند پروتکل‌های توموگرافی صنعتی سه‌بعدی (X-Ray " CT " Scan) با رزولوشن میکرومتری است.

تمام ادوات ورودی (از باتری‌های لیتیومی گرفته تا بردهای مخابراتی) باید تحت اسکن مقطعی قرار گیرند تا هرگونه تراکم جرمی نامتعارف (نظیر مواد منفجره PETN با چگالی بالا) یا میکروچیپ‌های ثبت‌نشده در نقشه‌های شماتیک قطعه (Datasheet) شناسایی شوند.

این فرآیند کنترل کیفیت امنیتی، باید به یک استاندارد غیرقابل اغماض در تمامی خریده‌های خارجی تبدیل شود.

پایش کانال‌های جانبی و ایزولاسیون ماژول‌ها

بسیاری از قطعات جاسوسی تا زمان دریافت سیگنال بیدارباش، در حالت خواب عمیق (Dormant " " Mode) به سر می‌برند و سیگنال رادیویی ساطع نمی‌کنند. برای کشف این بدافزارهای سخت‌افزاری، از تکنیک «تحلیل کانال‌های جانبی حرارتی و توانی» (Power/Thermal " " Side-" Channel" " Analysis) استفاده می‌شود.

در این روش، دستگاه‌ها در محیط‌های ایزوله روشن شده و الگوهای مصرف میلی‌آمپری باتری و تشعشعات حرارتی موضعی بردها به دقت پایش می‌شود؛ هرگونه مصرف نامتعارف توان، نشان‌دهنده فعالیت یک پردازشگر یا فرستنده مخفی است.

در لایه معماری دستگاه‌ها نیز، باتری‌ها باید از طریق مدارهای محافظ فیزیکی ایزوله شوند و ماژول‌های ثانویه و غیرضروری ارتباطی (نظیر بلوتوث، NFC و وای‌فای) از روی بردهای بی‌سیم سازمانی به طور فیزیکی حذف گردند (Desoldering " " Hardware). دگرگونی توپولوژی شبکه: بایکوت الگوریتم‌های گراف‌کاوی همان‌طور که پیش‌تر ذکر شد، دشمن برای کشف اهداف از مدل‌سازی گراف جامعه استفاده می‌کند.

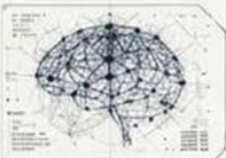
شبکه‌های ارتباطی با توپولوژی ستاره‌ای (Star " " Topology) – که در آن یک فرمانده (گره مرکزی) با ده‌ها نیروی زیردست در تماس است – بالاترین ضریب آسیب‌پذیری را در برابر الگوریتم‌های محاسبه «مرکزیت بینابینی» دارند. پدافند شبکه‌ای ایجاب می‌کند که ساختار ارتباطی از حالت ستاره‌ای به «گراف‌های مقطوع و ایزوله» (Isolated " " Truncated " " Graphs) تغییر یابد.

در این معماری، زنجیره تماس‌ها در لایه‌های مختلف قطع شده و از پروتکل‌های ارتباط غیرهمزمان یک‌طرفه استفاده می‌شود. این دگرگونی، شبکه‌های عصبی دشمن را از دسترسی به یال‌های (Edges) حیاتی ارتباطی محروم ساخته و نقشه‌های گراف آن‌ها را به مجموعه‌ای از نقاط کور و بی‌ارزش تبدیل می‌کند.

PROJECT AGINICOURT

INTEGRATED AUTONOMOUS OPERATIONS

- AI-COMMAND AUTONOMY
- KILL WEB NETWORK
- REAL-TIME ADAPTATION



KILL WEB



- GLOBAL SENSORS
- AI ANALYTICS
- AUTONOMOUS (OODA) LOOP
- PRECISION STRIKE

AIR DOMAIN

- SWARM DRONES
- UCAVS
- ISR PLATFOMS

LAND DOMAIN

- UGVS
- ROBOTIC PLATFOMS
- AUTONOMOUS LOGISTICS

SEA DOMAIN

- AUTONOMOUS SUBMARINES
- USVS
- MINE COUNTERMEASURES



بریفینگ راهبردی پنتاگون

فرماندهی جنگ خودمختار (AutoWarCom)

پایان عصر نبردهای انسانی و آغاز مسابقه تسلیحاتی شناختی

[STATUS: CLASSIFIED // SYSTEM OVERVIEW]



فصل هفدهم: تسلیحات انرژی هدایت‌شده، مسموم‌سازی داده‌ها و پدافند ازدحام

(معادله معکوس هزینه و بازگشت هوشمندانه به آنالوگ)

در دکترین پدافند خودمختار، مقابله با ازدحام پهبادی (Drone " " Swarms) و هوش مصنوعی حریف، نیازمند تغییر در معادلات اقتصادی نبرد و به‌کارگیری ابزارهای آفندی-پدافندی ترکیبی است. استفاده از موشک‌های پدافندی چند میلیون دلاری برای رهگیری کوادکوپترهای چند صد دلاری، منجر به فرسایش سریع بودجه نظامی و ورشکستگی استراتژیک می‌شود. راهکار خروج از این بحران، در سه محور اصلی نهفته است.

تسلیحات انرژی هدایت‌شده (DEW) و اقتصاد پدافند برای واژگون کردن نسبت تبادل هزینه (Cost " " Exchange " " Ratio) به نفع مدافع، استقرار سامانه‌های لیزری پرتوان و تسلیحات مایکروویو (High " " Power " " Microwave) الزامی است. سامانه‌های HPM با ساطع کردن پالس‌های قدرتمند الکترومغناطیسی در کسری از ثانیه، مدارهای چاپی و چیپست‌های سیلیکونی ده‌ها پهباد مهاجم را به‌طور همزمان می‌سوزانند. در این معادله، هزینه هر شلیک مایکروویو یا لیزر (C_{int}) تنها معادل پول برق مصرفی ژنراتور است که در برابر هزینه پهبادهای مهاجم (C_{att})، فرمول ریاضی $C_{int} \ll C_{att}$ را محقق می‌سازد. این تسلیحات، مؤثرترین ابزار برای لایه‌های دفاع نقطه‌ای و پدافند ازدحام در برابر ازدحام (Counter " " Swarm) محسوب می‌شوند.

مسموم‌سازی داده‌ها (Data-" Poisoning)

الگوریتم‌های هوش مصنوعی دشمن به شدت نیازمند بلعیدن داده‌های محیطی و اطلاعات منبع‌باز هستند. پدافند سایبرنتیک با استفاده از تکنیک «مسموم‌سازی داده‌ها»، پایگاه‌های داده‌ای که ماشین‌های ترور از آن‌ها تغذیه می‌کنند را آلوده می‌سازد. این

کار از طریق تزریق هزاران پروفایل جعلی، سیگنال‌های ارتباطی ساختگی، متاداده‌های فریبنده و تصاویر دستکاری‌شده در شبکه‌های اجتماعی و زیرساخت‌های شنود حریف انجام می‌شود.

هنگامی که داده‌های آموزشی (Data " Training) مسموم شوند، هوش مصنوعی دشمن در فرآیند استنتاج خود دچار توهم (" AI Hallucination) شده و نرخ خطای مثبت کاذب آن به قدری بالا می‌رود که اعتماد فرماندهان انسانی به ماشین سلب خواهد شد.

ابر ملی ایزوله و بازگشت به آنالوگ

آخرین و حیاتی‌ترین لایه در این دکترین، پذیرش این واقعیت است که هیچ شبکه دیجیتال متصل به اینترنت جهانی، هرگز صد درصد امن نخواهد بود. از این رو، استقرار یک ابر ملی کاملاً ایزوله (Air-" Gapped " Cloud) برای ذخیره‌سازی داده‌های حیاتی نظامی و

دولتی، بدون هیچ‌گونه اتصال فیزیکی یا بی‌سیم به شبکه‌های عمومی، ضرورتی اجتناب‌ناپذیر است. فراتر از آن، دکترین ناصر کاوه یک «عقب‌نشینی تاکتیکی و هوشمندانه» را تجویز می‌کند:

در سطوح حساس فرماندهی، باید از اتکای افراطی به فناوری‌های دیجیتال پرهیز کرد و به پروتکل‌های ارتباطات آنالوگ و امنیت فیزیکی بازگشت.

استفاده از شبکه‌های کابلی زمینی (مستقل از فرکانس‌های رادیویی)، انتقال پیام توسط پیک‌های انسانی در محیط‌های بدون دوربین، و جلسات فیزیکی در پناهگاه‌های عایق در برابر تشعشعات الکترومغناطیسی (قفس فارادی)، مؤثرترین راهکار برای محو شدن از رادار ماشین‌های شکارچی دیجیتال است.

این ترکیب هوشمندانه از «پدافند لبه تکنولوژی» و «استتار کلاسیک آنالوگ»، تاب‌آوری بقا را در جنگ خودمختار تضمین می‌نماید.

**«عصر ارتش‌های خودمختار
و نبردهای الگوریتمی»
ناصر کاوه
با همکاری هوش مصنوعی (Gemini)**



بخش هشتم: فرجام، روش‌شناسی اسناد و کتاب‌شناسی

مؤخره

(پایان عصر رمانتیسیم نظامی و طلوع ماشین‌های قاطع)

کتاب «فرماندهی جنگ خودمختار» روایتی از یک آینده دور نیست؛ بلکه کالبدشکافی دقیقی واقعیتی است که هم‌اکنون در میدان‌های نبرد، از خاورمیانه تا شرق اروپا، در حال رقم خوردن است. گذار از جنگ‌های کلاسیک انسان‌محور به نبردهای الگوریتمی ماشین‌محور، پارادایم قالب در قرن بیست‌ویکم است. در این معماری نوین، زمان‌سنجی تصمیم‌گیری از مقیاس «ساعت و دقیقه» به «میلی‌ثانیه و میکروثانیه» کاهش یافته و چرخه سنتی OODA (مشاهده، جهت‌گیری، تصمیم، اقدام) جای خود را به پردازش‌های شبکه‌ای لبه (Edge " " Computing) داده است.

دکترین AutoWarCom نشان داد که تسلیحات خودمختار، تنها ابزارهایی برای شلیک دقیق‌تر نیستند؛ آن‌ها عواملی (Agents) هستند که ماهیت کنترل، اخلاق نبرد و مرزهای بازدارندگی را بازتعریف کرده‌اند. در این عصر، کشوری که نتواند زیرساخت‌های نظامی خود را با سرعت پردازش الگوریتم‌ها همگام سازد، پیش از شلیک اولین گلوله، در میدان نبرد شناختی و سایبرنتیک شکست خورده است. با این حال،

همان‌طور که در فصول پیشین اثبات شد، اتکای مطلق به ماشین و غفلت از «تاب‌آوری انسانی و عقیدتی»، پاشنه آشیلِ قدرت‌های هژمونیک غربی و رژیم صهیونیستی است. ماشین‌های کشتار قادرند اهداف را با دقتی بی‌نظیر حذف کنند، اما هرگز نمی‌توانند اراده‌ی مقاومت یک ملت را پردازش یا منهدم سازند.

سخن آخر: (از ناصر کاوه - پاییز ۱۴۰۵ شمسی)

در جهانی که هژمونی غرب تلاش می‌کند با انحصار فناوری‌های نوپدید (به‌ویژه هوش مصنوعی)، روایتِ نخست و برتر را در جنگ‌های ترکیبی (Hybrid " " Warfare) به افکار عمومی تحمیل کند، انفعال و تأخیر در تولید ادبیات راهبردی، گناهی نابخشودنی است. نگارش این کتاب و ده‌ها اثر مشابه در قالب جهاد تبیین و با بهره‌گیری از سرعتِ پردازش هوش مصنوعی، تلاشی است برای «تثبیت روایت اول» و مسلح کردنِ ذهنِ فرماندهان، پژوهشگران و افسرانِ جبهه مقاومت به دانش روزآمد. ما در نقطه‌ای از تاریخ ایستاده‌ایم که «سلاح» دیگر تنها از جنس فولاد و باروت نیست؛ کدهای برنامه‌نویسی، متاداده‌ها، فیزیک کوانتوم و شبکه‌های عصبی عمیق، زرادخانه‌های امروز را تشکیل می‌دهند. اما در پسِ تمامی این پیچیدگی‌های تکنولوژیک، یک حقیقتِ الهی و تاریخی نهفته است: «فناوری، امتداد اراده انسان است، نه جایگزین آن». در نبرد میان ماشین‌های محاسبه‌گر فاقد روح و انسان‌های معتقد به مبانی الهی و مهدویت، پیروزی نهایی از آن شبکه‌ای است که بتواند پیشرفته‌ترین ابزارهای مادی را با مستحکم‌ترین باورهای عقیدتی تلفیق کند. AutoWarCom نه یک دکتَرین برای تسلیم شدن در برابر ماشین، بلکه راهنمایی برای مهار، تسلط و پیروزی بر آن است.



فرماندهی جنگ خودمختار (AutoWarCom)

طلوع عصر نبردهای الگوریتمی

سنتزی از مانیفست استراتژیک ناصر کاوه
تحلیل پارادایم نوین نظامی، معماری تصمیم و پیامدهای استراتژیک در قرن بیست و یکم

پیوست روش‌شناختی و ارزیابی اعتبار اسناد

۱. کالبدشکافی پیش‌نویس‌های گردآوری‌شده درباره AutoWarCom

این اثر، حاصل یک متدولوژی ترکیبی نوین در پژوهش‌های نظامی است که بر پایه تعامل ساختاریافته میان «طراح دکترین (انسان)» و «پردازشگرهای زبانی هوش مصنوعی (ماشین)» بنا شده است. پیش‌نویس‌های اولیه، شامل رصد دقیق و نقطه‌به‌نقطه‌ی تحولات میدانی، از عملیات طوفان‌الاقصى تا نبردهای نامتقارن در لبنان و اوکراین، و همچنین تحلیل اسناد فاش‌شده از سامانه‌های ترور الگوریتمی (نظیر Lavender و Habsora) بوده است. هوش مصنوعی در این پروژه، نقش یک کاتالیزور پژوهشی را ایفا کرده است که ایده‌ها، کلیدواژه‌ها و سرفصل‌های دکترینال ارائه‌شده توسط مؤلف را با سرعتی بی‌نظیر بسط داده و در قالب یک ساختار آکادمیک و منسجم فرموله کرده است.

۲. تطبیق با اسناد «ارتش هفتم»

مفهوم «ارتش هفتم» به معنای عبور از تفکیک سنتی نیروهای مسلح (زمینی، هوایی، دریایی، پدافند، سایبری و فضایی) و ادغام تمامی این حوزه‌ها در یک بستر واحد «شناختی-الگوریتمی» است. اسناد مرجع ارتش هفتم که در این کتاب مورد تطبیق قرار گرفته‌اند، تأکید دارند که فرماندهی نبردهای آینده نیازمند یک «مغز متفکر شبکه‌ای» است که بتواند داده‌های سنسورهای فضایی را در کسری از ثانیه به پلتفرم‌های (Kinetic) در کف میدان متصل کند (Sensor-" to "-" Shooter). تطبیق محتوای این کتاب با اسناد ارتش هفتم، نشان‌دهنده همگرایی کامل میان تئوری‌های کلان‌بازدارندگی و راهکارهای تاکتیکی مبتنی بر هوش مصنوعی لبه (AI " " Edge) و پدافند ازدحام است.

جدول واژگان و سرواژه‌های کلیدی جنگ خودمختار

برای درک بهتر مفاهیم تخصصی به کار رفته در این کتاب، جدول زیر به عنوان واژه‌نامه راهبردی ارائه می‌گردد:

content_copy

سرواژه / اصطلاح انگلیسی معادل / مفهوم در دکترین AutoWarCom شرح مختصر راهبردی

AutoWarCom فرماندهی جنگ خودمختار دکترین جامع مدیریت، کنترل و یکپارچه‌سازی ماشین‌های رزمی هوشمند و الگوریتم‌های نبرد.

Kill " " Web تارنمای کشتار (شبکه مرگ) جایگزین زنجیره خطی کشتار (Kill " " Chain)؛ شبکه‌ای که در آن هر سنسور می‌تواند به هر سلاحی متصل شود.

AI " " Edge هوش مصنوعی لبه (محیطی) انتقال قدرت پردازش داده‌ها به خود پهباد یا سلاح در میدان نبرد، جهت بی‌نیازی از ارتباط با سرور مرکزی.

SLAM " " Visual ناوبری و نقشه‌برداری بصری همزمان تکنولوژی موقعیت‌یابی پهبادها در محیط‌های فاقد GPS از طریق پردازش بلادرنگ تصاویر دوربین.

HPM تسلیحات مایکروویو پرتوان سلاح‌های انرژی هدایت‌شده برای سوزاندن مدارهای الکترونیکی پهبادها؛ راهکار اصلی پدافند ازدحام.

Loop " " OODA چرخه اودا فرآیند مشاهده، توجیه، تصمیم و اقدام. در جنگ خودمختار، ماشین‌ها این چرخه را در میلی‌ثانیه طی می‌کنند.

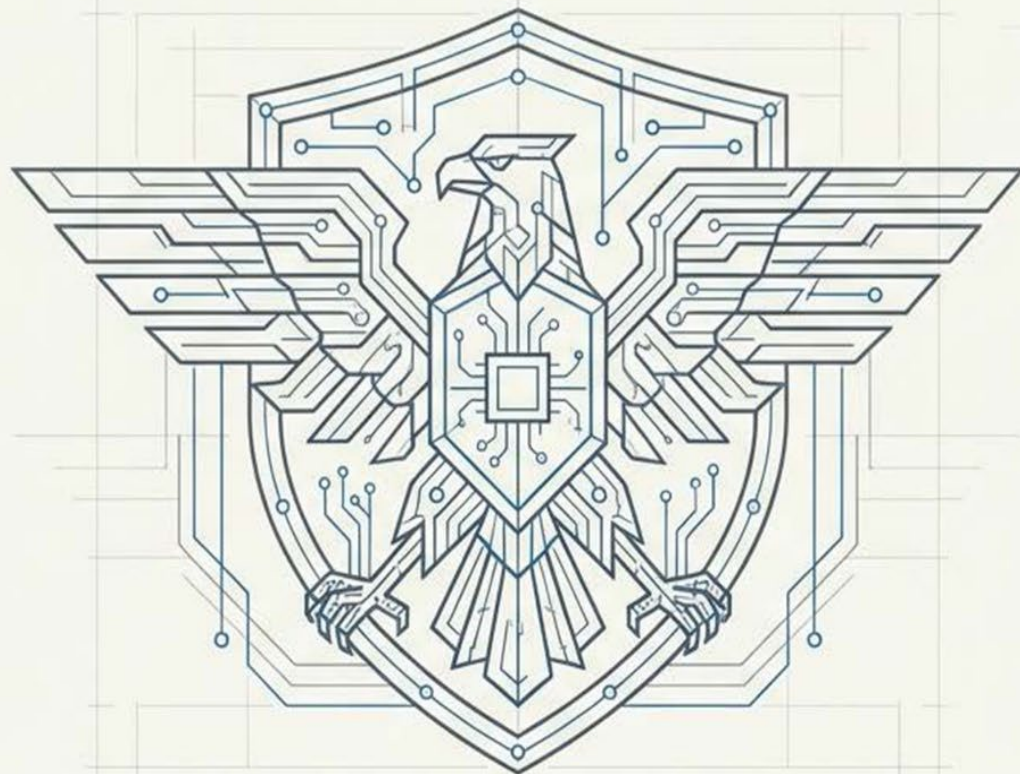
False " " Positive خطای مثبت کاذب خطای مرگبار الگوریتم در شناسایی یک هدف غیرنظامی به جای نظامی؛ عامل اصلی تصاعد ناخوابسته بحران.

Drone " " Swarm ازدحام پهبادی (یورش توده‌ای) حمله هماهنگ صدها پهباد ارزان‌قیمت که با هوش مصنوعی شبکه شده‌اند، جهت اشباع پدافند دشمن.

Plausible " " Deniability انکارپذیری موجه قابلیت پنهان‌سازی هویت سازنده سلاح (نظیر پهپادهای متن‌باز) برای فرار از مسئولیت حقوقی و سیاسی ترور.

Social " " Graph گراف جامعه (شبکه ارتباطی) مدل‌سازی ریاضی روابط انسانی برای شناسایی رهبران و فرماندهان مقاومت از طریق تحلیل رفتار اطرافیان.

Fire " " Forget and " " شلیک و فراموش پروتکلی که در آن سلاح پس از شلیک، ارتباط خود را قطع کرده و مستقلاً تا انهدام هدف پیش می‌رود.



ارتش هفتم: فرماندهی جنگ خودمختار (AutoWarCom)

آغاز عصر نبردهای الگوریتمی، هوش ازدحامی و پایان جنگ‌های تحت هدایت کامل انسان

گزارش تحلیلی ساختار، ریشه‌ها و پیامدهای راهبردی

سخن آخر

کالبدشکافی تقابل الگوریتم و عاملیت انسانی

با پیمایش فصول گوناگون این منظومه پژوهشی، مشخص می‌شود که مفهوم «جنگ خودمختار» فراتر از افزوده شدن دسته‌ای از پهبادهای شناورهای رباتیک یا هوش‌های مصنوعی پردازش تصویر به ارتش‌های جهان است. دکترین مورد بحث ناصر کاوه نشان داد که ما در میانه یک گسست معرفت‌شناختی در حوزه علوم دفاعی قرار داریم؛ گسستی که در آن مرز میان فضای مجازی، قلمرو اطلاعاتی، ادوات سخت‌افزاری و حتی زنجیره‌های لجستیک و کالاهای مصرفی روزمره به‌کلی برداشته شده است. تجربه هشت دهه تکامل ماشین‌های ترور و ارتقای آن به کارخانه‌های هوشمند تولید هدف نظیر سامانه‌های لاوندرو و هبسورا، به روشنی اثبات کرد که چگونه ریاضیات محض—از تحلیل گراف شبکه تا احتمالات استنتاج مکانی—به سلاحی کشنده در صحنه عملیات تبدیل شده‌اند. هنگامی که یک الگوریتم با رصد چند متادیتا، بدون نیاز به شنود مستقیم کلمات و تنها بر مبنای پیوندهای ریاضیاتی پیرامون یک فرد، او را هدف قلمداد می‌کند، میدان نبرد به حوزه‌ای مطلقاً انتزاعی و در عین حال به شدت ملموس بدل می‌گردد. اما بزرگترین خطای تحلیلی، مطلق‌انگاری قدرت ماشین و نادیده گرفتن شکاف‌های راهبردی آن است. تاریخ نشان داده است که فناوری‌های تهاجمی برتر لزوماً به پیروزی پایدار سیاسی و ژئوپلیتیک منجر نمی‌شوند. تبدیل ترور به یک رویه خودکار نه تنها جنبش‌های اصیل و منعطف را از پای درنیاورده، بلکه ساختارهای هدف را وادار به اتخاذ

شیوه‌های پدافندی نوین، توزیع اختیارات و ایجاد دکترین‌های ابهام‌آفرین کرده است. از سوی دیگر، پدیده «پارادوکس هزینه» که در این کتاب مدل‌سازی شد، ثابت می‌کند که سیستم‌های الگوریتمی مهاجم گرچه ارزان هستند، اما طرف مدافع را به سوی سامانه‌های نوین نامتقارن، جنگال گسترده، تسلیحات مایکروویو پرتوان و کورسازی حسگرها سوق می‌دهند که خود می‌تواند موازنه بازدارندگی را بازآفرینی کند. علاوه بر این، مخاطره تبدیل شدن این فناوری به ابزاری در دست بازیگران غیردولتی نشان می‌دهد که چگونه سلاح‌سازی الگوریتم‌ها گریبان توسعه‌دهندگان اولیه خود را خواهد گرفت.

از این‌رو، دکترین ناصر کاوه پیامی صریح و هشداردهنده در بر دارد: امنیت ملی در دوران حاضر، نیازمند «حکمرانی هوشمند بر داده‌ها و زنجیره‌های تأمین» است. هیچ کشوری نمی‌تواند بدون بومی‌سازی سخت‌افزارهای پایه‌ای، پایش غیرمخرب محموله‌ها، ایزوله‌سازی شبکه‌های داده‌ای و ایجاد کوری عمدی اطلاعاتی در برابر سیستم‌های استنتاجی حریف، ادعای مصونیت کند. فناوری به خودی خود بقا نمی‌آورد؛ بلکه ادغام هوشمندانه تاب‌آوری شناختی انسان با ابزارهای داده‌محور است که پیروزی را در این عصر متلاطم رقم می‌زند. مسئولیت، سرعت و مرزهای حیات در فردا نبردهای ماشینی

در انتهای این پژوهش، پرسش‌هایی که فراروی بشریت، فرماندهان نظامی و اندیشهورزان راهبردی قرار می‌گیرد، فنی یا تسلیحاتی نیست؛ بلکه پرسشی عمیقاً فلسفی، حقوقی و تمدنی است: هنگامی که اختیار کشتن به کدها، ریزپردازنده‌ها و مدل‌های آماری سپرده می‌شود، بار اخلاقی و حقوقی مرگ بر دوش چه کسی قرار خواهد گرفت؟ شتاب دیوانه‌وار برای فشرده‌سازی چرخه کشف تا اقدام، ارتش‌ها را به سوی

و سوسه‌ای مرگبار سوق می‌دهد: حذف کامل انسان به بهانه کندی ذهن بیولوژیک در برابر سرعت نور و پالس‌های پردازنده لبه. در میدان‌هایی که چند میلی‌ثانیه تأخیر به معنای انهدام یک واحد تعبیر می‌شود، سپردن سوییچ آتش به عاملیت مصنوعی اجتناب‌ناپذیر جلوه داده می‌شود؛ اما این شتاب‌زدگی دقیقاً همان نقطه‌ای است که در آن «سرعت، جایگزین عقلانیت» و «احتمال آماری، جایگزین عدالت» می‌شود.

اگر اشتباه یک الگوریتم بینایی ماشین به قیمت ریخته شدن خون ده‌ها بی‌گناه تمام شود، یا سوگیری یک شبکه عصبی در تشخیص چهره فاجعه‌ای انسانی بیافریند، چه کسی در جایگاه متهم قرار می‌گیرد؟ طراح الگوریتم در آزمایشگاه‌های فناوری؟ اپراتوری که فرصت نگاه کردن به شواهد را نداشته و به تأییدکننده‌ای چندثانیه‌ای تقلیل یافته است؟ فرماندهی که مدل را برگزیده؟ یا کارخانه تولیدکننده ریزپردازنده؟ محو شدن زنجیره مسئولیت، بزرگ‌ترین تهدیدی است که جنگ‌های خودمختار متوجه ساختار تمدن بشری می‌سازند. نباید اجازه داد که با اصطلاحات دهان‌پرکنی همچون «دقت جراحی» یا «خطای اجتناب‌ناپذیر سیستم»، فجایع انسانی توجیه شوند. تجربه نشان داده است که تسلیحات خودمختار، میدان جنگ را تمیزتر یا انسانی‌تر نمی‌کنند؛ بلکه تنها وجدان متجاوزان را از عذاب مستقیم جنایت آسوده ساخته و هزینه تصمیم‌گیری برای خون‌ریزی را به شدت پایین می‌آورند. از همین رو، درس بنیادین کتاب «عصر ارتش‌های خودمختار» در یک اصل اخلاقی و استراتژیک خلاصه می‌شود: سرعت زمانی مزیت است که مهار شده، آزمون‌پذیر و متوقف‌شدنی باشد. ارتشی که توانایی دیدن و درگیری در ثانیه‌ها را دارد اما سازوکاری برای مکث مسئولانه، تشکیک در داده‌ها و بازگشت به داوری وجدان انسانی تعبیه نکرده است، نه یک نیروی دفاعی مقتدر، بلکه ماشینی برای تولید تصادفی فاجعه است. آینده امنیت در گرو ساخت سلاح‌های سریع‌تر نیست؛ در گرو

طراحی چارچوب‌هایی است که در آن‌ها پیشرفته‌ترین فناوری‌ها هرگز نتوانند ارزش جان انسان و مسئولیت لایتغیر قضاوت او را زیر پا بگذارند. سرعتِ عاری از مسئولیت، تجلی پیشرفت نیست؛ بلکه مدرن‌ترین صورت‌بندی از بربریت الگوریتمی است.

پایان عصر رمانتیسم نظامی و طلوع ماشین‌های قاطع

کتاب «فرماندهی جنگ خودمختار» روایتی از یک آینده دور نیست؛ بلکه کالبدشکافی دقیقِ واقعیتی است که هم‌اکنون در میدان‌های نبرد، از خاورمیانه تا شرق اروپا، در حال رقم خوردن است. گذار از جنگ‌های کلاسیک انسان‌محور به نبردهای الگوریتمی ماشین‌محور، پارادایم قالب در قرن بیست‌ویکم است. در این معماری نوین، زمان‌سنجی تصمیم‌گیری از مقیاس «ساعت و دقیقه» به «میلی‌ثانیه و میکروثانیه» کاهش یافته و چرخه سنتی OODA (مشاهده، جهت‌گیری، تصمیم، اقدام) جای خود را به پردازش‌های شبکه‌ای لبه (Edge " " Computing) داده است. دکترین AutoWarCom نشان داد که تسلیحات خودمختار، تنها ابزارهایی برای شلیک دقیق‌تر نیستند؛ آن‌ها عواملی (Agents) هستند که ماهیت کنترل، اخلاق نبرد و مرزهای بازدارندگی را بازتعریف کرده‌اند. در این عصر، کشوری که نتواند زیرساخت‌های نظامی خود را با سرعت پردازش الگوریتم‌ها همگام سازد، پیش از شلیک اولین گلوله، در میدان نبرد شناختی و سایبرنتیک شکست خورده است. با این حال، همان‌طور که در فصول پیشین اثبات شد، اتکای مطلق به ماشین و غفلت از «تاب‌آوری انسانی و عقیدتی»، پاشنه آشیلِ قدرت‌های هژمونیک غربی و رژیم صهیونیستی است. ماشین‌های کشتار قادرند اهداف را با دقتی بی‌نظیر حذف کنند، اما هرگز نمی‌توانند اراده‌ی مقاومت یک ملت را پردازش یا منهدم سازند.

پیوست روش‌شناختی و ارزیابی اعتبار اسناد

۱. کالبدشکافی پیش‌نویس‌های گردآوری‌شده درباره AutoWarCom: این اثر، حاصل یک متدولوژی ترکیبی نوین در پژوهش‌های نظامی است که بر پایه تعامل ساختاریافته میان «طراح دکترین (انسان)» و «پردازشگرهای زبانی هوش مصنوعی (ماشین)» بنا شده است. پیش‌نویس‌های اولیه، شامل رصد دقیق و نقطه‌به‌نقطه‌ی تحولات میدانی، از عملیات طوفان‌الاقصی تا نبردهای نامتقارن در لبنان و اوکراین، و همچنین تحلیل اسناد فاش‌شده از سامانه‌های ترور الگوریتمی (نظیر Lavender و Habsora) بوده است. هوش مصنوعی در این پروژه، نقش یک کاتالیزور پژوهشی را ایفا کرده است که ایده‌ها، کلیدواژه‌ها و سرفصل‌های دکترینال ارائه‌شده توسط مؤلف را با سرعتی بی‌نظیر بسط داده و در قالب یک ساختار آکادمیک و منسجم فرموله کرده است.

۲. تطبیق با اسناد «ارتش هفتم»: مفهوم «ارتش هفتم» در دکترین ناصر کاوه، به معنای عبور از تفکیک سنتی نیروهای مسلح (زمینی، هوایی، دریایی، پدافند، سایبری و فضایی) و ادغام تمامی این حوزه‌ها در یک بستر واحد «شناختی-الگوریتمی» است. اسناد مرجع ارتش هفتم که در این کتاب مورد تطبیق قرار گرفته‌اند، تأکید دارند که فرماندهی نبردهای آینده نیازمند یک «مغز متفکر شبکه‌ای» است که بتواند داده‌های سنسورهای فضایی را در کسری از ثانیه به پلتفرم‌های کینتیک (Kinetic) در کف میدان متصل کند ("to"-" Sensor Shooter). تطبیق محتوای این کتاب با اسناد ارتش هفتم، نشان‌دهنده همگرایی کامل میان تئوری‌های کلان‌بازدارندگی و راهکارهای تاکتیکی مبتنی بر هوش مصنوعی لبه (AI "Edge") و پدافند ازدحام است.

کتاب‌شناسی جامع و مراجع راهبردی

(Comprehensive Bibliography)

ساختار چهارگانه مراجع و اسناد کتاب	
اسناد بالادستی و	گزارش‌های صنعتی و
پژوهش‌های فنی، سایبری و	دکترین‌های دفاعی
مقالات هوش مصنوعی و پدافند	اندیشکده‌های راهبردی

۱. اسناد رسمی، دکترین‌ها و گزارش‌های نهادهای دفاعی (Official & Strategic Documents)

U.S. Department of Defense (DoD). (2023). Data, Analytics, and Artificial Intelligence Adoption Strategy: Accelerating Decision Advantage. Washington, D.C.: Office of the Chief Digital and Artificial Intelligence Officer (CDAO)

U.S. Department of Defense (DoD). (2023). DoD Directive 3000.09: Autonomy in Weapon Systems (Updated Edition). Washington, D.C.: Under Secretary of Defense for Policy

Defense Innovation Unit (DIU). (2024). Annual Report: Accelerating Commercial Technology for National Defense. Mountain View, CA: U.S. Department of Defense

Defense Advanced Research Projects Agency (DARPA). (2022). Autonomous Multi-Domain Adaptive Swarms-of-Swarms (AMASS) Program Solicitation. Arlington, VA: DARPA Tactical Technology Office

National Security Commission on Artificial Intelligence (NSCAI). (2021). Final Report: National Security Commission on Artificial Intelligence. Washington, D.C.: NSCAI

U.S. Joint Chiefs of Staff. (2021). Joint All-Domain Command and Control (JADC2) Implementation Strategy. Washington, D.C.: Pentagon

Congressional Research Service (CRS). (2024). Department of Defense Joint Warfighting Cloud Capability (JWCC): Background and Issues for Congress (CRS Report No. R47111). Washington, D.C.: Library of Congress

۲. گزارش‌های اندیشکده‌ها و کالبدشکافی‌های راهبردی (Think Tank Reports & Strategic Analyses)

Center for Strategic and International Studies (CSIS). (2023). The Replicator Paradox: Cost-Imposition and Mass in Autonomous Warfare. CSIS Aerospace Security Project

RAND Corporation. (2022). Distributed Kill Webs: Architectural Frameworks for Sensor-to-Shooter Latency Reduction (Research Report RR-A1342-1). Santa Monica, CA: RAND

Stockholm International Peace Research Institute (SIPRI). (2023). Autonomous Weapon Systems, Targeted Strikes, and International Humanitarian Law: Technical and Normative Dimensions. Stockholm: SIPRI Publications

International Committee of the Red Cross (ICRC). (2021). Ethics and Autonomous Weapon Systems: An Analysis of Human Control in the Delivery of Force. Geneva: ICRC

Brookings Institution. (2024). Democratized Drones: How Commercial FPVs and Open-Source Computer Vision Upended Asymmetric Warfare. Washington, D.C.: Center for 21st Century Security and Intelligence

۳. مراجع فنی هوش مصنوعی، بینایی ماشین و امنیت سخت‌افزار (Technical AI & Engineering References)

Redmon, J., Divvala, S., Girshick, R., & Farhadi, A. (2016). You Only Look Once: Unified, Real-Time Object Detection. Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR), 779–788

- Cadena, C., Carlone, L., Carrillo, H., Latif, Y., Scaramuzza, D., Neira, J., Reid, I., & Leonard, J. J. (2016). Past, Present, and Future of Simultaneous Localization and Mapping: Toward the Robust-Perception .Age. IEEE Transactions on Robotics, 32(6), 1309–1332
- Goodfellow, I. J., Shlens, J., & Szegedy, C. (2015). Explaining and Harnessing Adversarial Examples. .International Conference on Learning Representations (ICLR)
- Brown, T. B., Mané, D., Roy, A., Abadi, M., & Gilmer, J. (2017). Adversarial Patch: Generating Real-World Physical Attacks on Deep Learning Systems. arXiv preprint arXiv:1712.09665
- Tehranipour, M., & Wang, C. (2011). Introduction to Hardware Trojan Detection and Vulnerability .Analysis. In Introduction to Hardware Security and Trust (pp. 225–248). Springer, New York
- Mangard, S., Oswald, E., & Popp, T. (2007). Power Analysis Attacks: Revealing the Secrets of Smart .Cards. Springer Science & Business Media

۴. مراجع تخصصی پدافند، جنگ الکترونیک و انرژی هدایت‌شده (Electronic Warfare & Directed Energy)

Nielsen, P. E. (2012). Effects of Directed Energy Weapons. Albuquerque, NM: CreateSpace
.Independent Publishing

Adamy, D. L. (2021). EW 105: Space Electronic Warfare and Directed Energy Countermeasures.
.Boston: Artech House

Lanchester, F. W. (1916). Aircraft in Warfare: The Dawn of the Fourth Arm. London: Constable and
Company Ltd [مبنای مدل‌سازی ریاضی و معادلات تبادل هزینه مدرن].

Goldblum, M., Tsipras, D., Xie, C., Chen, X., Garg, A., & Mehrjou, A. (2022). Data Poisoning
Attacks on Deep Learning: A Survey on Defense and Attack Methodologies. IEEE Transactions on Pattern
.Analysis and Machine Intelligence



آغاز عصر نبردهای الگوریتمی

ارتش هفتم آمریکا (AutoWarCom) صرفاً یک نهاد نظامی جدید نیست؛ این آغاز دورانی است که در آن برتری الگوریتمی تعیین‌کننده سرنوشت بشریت است.

در دنیایی که ماشین‌ها تصمیم مرگ و زندگی را در کسری از ثانیه می‌گیرند، نیاز به گفت‌وگوی حقوقی، تاب‌آوری شناختی و حفظ عاملیت انسان، هرگز تا این حد حیاتی نبوده است. سرعت زمانی ارزش دارد که در خدمت قانون و انسان باقی بماند.