



خبرنامه

(۳)

سال سوم

آذرماه - ۱۴۰۱

مرکز خدمات ویژه دفاعی

۱۰۱

"خبرنامه دفاعی"

۱۰۱ - ویک - ۱۰۱ - ۱۰۱

۱۰۱

امور بین المللی وزارت دفاع و پشتیبانی نیروهای مسلح



۱- اهمیت اینترنت اشیا و هوش مصنوعی در نبردهای آینده.

۲- رقابت آمریکا و چین بر سر هوش مصنوعی، تراشه ها و 5G.

۳- فناوری های مخرب نوظهور دفاعی.

۴- کاربرد هوش مصنوعی برای شناسایی اهداف توسط تانک جدید ارتش آمریکا.

۵- رمز گذاری کوانتومی ماهواره برای تقویت استقلال اروپا.

اهمیت اینترنت اشیاء و هوش مصنوعی در نبرد های آینده

در درگیری های آینده، تصمیم گیری های حیاتی بایستی در عرض چند ساعت یا چند ثانیه اتخاذ گردد. که این امر مستلزم تجزیه و تحلیل یک محیط عملیاتی و صدور فرمان است. یکی از راه هایی که برای سرعت بخشیدن و خود کار سازی تصمیم گیری در نظر گرفته می شود، اینترنت اشیاء نظامی (IOT) و هوش مصنوعی (AI) است. یکی از ابتکارات مهم وزارت دفاع آمریکا JADC2=Joint All Domain Command &Control جمع آوری جریان های داده از هزاران تجهیزات موجود در میدان نبرد، حسگرهای محیطی و سایر دستگاههای هوشمند در هر شاخه نظامی است. سپس می توان از هوش مصنوعی و یاد گیری ماشینی (ML) برای ارزیابی اطلاعات مرتبط استفاده کرد که امکان تصمیم گیری سریع در خطوط مقدم را حتی تا سطح شناسایی اهداف نظامی و توصیه بکارگیری سلاح بهینه برای درگیری فراهم می کند.

اینترنت اشیاء نظامی شامل موارد مختلفی از حساسه های میدان نبرد و سامانه های تسلیحاتی تا دستگاههای ردیابی، تجهیزات ارتباطی، فناوری های پوشیدنی، هواپیماهای بدون سرنشین، کشتی ها، هواپیماها، تانک ها و حتی حسگرهای متصل به بدن انسان می باشد که مجموعاً حجم عظیمی از اطلاعات برخط را به میدان جنگ ارسال می کنند. هر شاخه از ارتش، اینترنت اشیاء مختص به خود را دارد برای نیروی هوایی، اینترنت اشیاء جزء ضروری از سامانه مدیریت پیشرفته میدان نبرد یا (ABMS) است. برای نیروی زمینی، "فرماندهی آینده" و در نیروی دریایی، پروژه Overmatch مطرح است.

هدف کلی JADC2 این است که همه ابتکارات موجود را به هم پیوند دهد و آنها را به عنوان یک نیروی واحد و موفق در میدان بکار گیرد. موفقیت اینترنت اشیاء البته به توانایی جمع آوری و ذخیره حجم عظیمی از جریان داده از هزاران اشیاء به صورت در لحظه بستگی دارد. با این حال، یک چالش بزرگتر، درک آنی اطلاعات و رساندن نتایج به ادوات جنگی در زمان مناسب است به گونه ای که بتوانند از آن به نحو شایسته استفاده کنند.

اما موانع فنی بسیار زیادی در این مسیر وجود دارند که در ادامه به مهمترین آنها اشاره می شود:

۱- یکی از مشکلات، تلفیق وبه اشتراک گذاری حجم عظیمی از جریان داده های (IOT) تولید شده از سامانه های مستقر در یگان ها با قالب های متنوع داده و شبکه های ارتباطی مختلف است. در حالت مطلوب، بایستی داده و ذخیره سازی آن در قالب واحد باشد که بتواند به سرعت پردازش شود.

۲- عدم وجود یک شبکه مشترک با پهنای باند بالا و تاخیر کم که به عنوان شبکه مشترک دستگاههای (IOT) نظامی و محیط های پردازش و هوش مصنوعی عمل می کند. برای رفع این مشکل راه حل هایی از جمله استفاده از ماهواره و شبکه نظامی اختصاصی مطرح است. 5G توسط بسیاری از کارشناسان، به عنوان راه حل نهایی شناخته شده است. راهکار دیگر، ذخیره سازی انعطاف پذیر داده، ارتباطات، همگام سازی و پردازش در انتهای شبکه، حتی در مکان های دور یا در زمان هایی که هیچ قابلیت ارتباطی مانند 5G در دسترس نباشد، مورد نظر کارشناسان است.

وزارت دفاع آمریکا در مراحل اولیه برنامه ریزی و اجرای JADC2 و (IOT) است. با فرض اینکه بتوان برای چالش های اینترنت اشیا راهکار مناسبی پیدا کرد، چند نمونه از موارد استفاده از این فناوری در زیر آورده شده است:

۱- سامانه های تسلیحاتی خود مختار:

انسان همچنان عامل اصلی میدان نبرد است. با این حال، سامانه های نظارتی و تسلیحاتی مستقل مانند پهپادها، موشک های هوشمند و خودروهای بدون سرنشین، می توانند نظارت پیشرفته ای در میدان نبرد انجام دهند و اطلاعات نبرد را تقویت کنند و یا با اهداف درگیر شوند.

۲- حسگرها و تجهیزات سربازان:

اغلب حسگرها و تجهیزات سربازان، اینترنت اشیا میدان نبرد نامیده می شوند، شبکه ای از اطلاعات جمع آوری شده و حسگرهای "بیومتریک" بدن که در لباس های رزمی، کلاه ایمنی، سامانه های تسلیحاتی و وسایل نقلیه سربازان تعبیه شده اند، می توانند اطلاعات ارزشمند میدان نبرد را همراه با موقعیت سرباز و وضعیت سلامتی سربازان منتقل کنند.

۳- آگاهی از موقعیت:

آگاهی از موقعیت برای تصمیم‌گیری سریع و موثر در میدان نبرد حیاتی است. تلفیق اینترنت اشیاء با هوش مصنوعی نه تنها راهی برای افزایش آگاهی موقعیتی است، بلکه سرعت تصمیم‌گیری را نیز افزایش می‌دهد. موارد متعدد دیگری نیز برای استفاده از اینترنت اشیاء، مانند نظارت بر خودروهای میدان نبرد، امنیت پایگاه‌ها، نگهداری پیشگیرانه در میدان نبرد وجود دارد. هرچه که میدان جنگ پیچیده تر و غیر قابل پیش‌بینی می‌شود، اینترنت اشیاء و هوش مصنوعی به یک راهبرد با ارزش برای تسریع تصمیم‌گیری‌های حیاتی خودکار، درک وضعیت دشمن و به حداقل رساندن تلفات تبدیل خواهد شد.

رقابت آمریکا و چین بر سر هوش مصنوعی، تراشه ها و 5G

نتایج یک مطالعه ویژه در زمینه رقابت بین المللی در حوزه فناوری های نوظهور حاکی از آن است که چنانچه آمریکا در آینده در رقابت با چین بر سر توسعه فناوری های کلیدی مانند هوش مصنوعی شکست بخورد، آینده مبهمی در انتظار امنیت اقتصادی و نظامی آمریکا خواهد بود. در همین راستا معاون اسبق وزیر دفاع آمریکا (رابرت ورک) که رییس فعلی پروژه مطالعاتی فناوری های نوظهور آمریکا است، طی سخنانی اظهار داشته:

"اگر چین در رقابت های فناورانه با آمریکا به پیروزی دست یابد، می تواند از پیشرفت های خود در هوش مصنوعی و فناوری "بیو لوژیکی" برای تقویت بنیه اقتصادی و دفاعی کشور خود استفاده کند و از این طریق قادر به تهدید سایر کشور های جهان خواهد بود".

از نظر "رابرت ورک"، شکست در برابر چین به این معنی است که امنیت آمریکا مورد تهدید قرار خواهد گرفت. زیرا چین قادر به ایجاد یک نظارت جهانی خواهد شد و در این صورت شرکت های فناوری آمریکایی میلیارد ها دلار از دست خواهند داد و آمریکا برای فناوری های اصلی به چین یا سایر کشورهای تحت نفوذ چین متکی خواهد شد.

وی معتقد است اگر این اتفاق رخ دهد حوزه نفوذ چین با افزایش بسترهای فناورانه در سراسر جهان رشد خواهد کرد و آنها قادر خواهند بود نظارت فناورانه را در مقیاس جهانی برقرار کنند.

"اریک اشمیت" رییس مشترک پروژه مطالعات ویژه و مدیر عامل سابق شرکت "گوگل" نیز بر این باور است که رقابت بر سر فناوری، فراتر از درگیری یا تمرکز نظامی است. تمرکز چین برای پیروز شدن در این رقابت بر سر توسعه زیرساخت هاست. زیرا از نظر چینی ها در آینده نمی توان به زیر ساخت های تحت سلطه شرکت های غربی تکیه کرد.

گزارش ویژه پروژه مطالعات رقابتی بیان می دارد، جنگ آینده آمریکا و چین بر رقابت در سه حوزه هوش مصنوعی، تراشه ها و 5G متمرکز است. اهمیت ایجاد و توسعه این سه حوزه واقعا حیاتی است، زیرا این رقابت فقط مربوط به رقابت نظامی نیست بلکه در مورد تمام مزایایی است که هر سه حوزه مذکور برای اقتصاد و جامعه به ارمغان خواهد آورد و در نهایت ارتش نیز می تواند از آن استفاده کند.

آمریکا در حوزه 5G هنوز برنامه مناسبی برای رقابت با چین ندارد. به عنوان مثال می توان به یکی از غولهای فناوری چین یعنی شرکت "هوآوی" اشاره کرد که حدود ۷۰٪ از 4G آفریقا را در کنترل خود دارد. چین همچنین میلیاردها دلار برای تولید تراشه سرمایه گذاری کرده است و در حوزه هوش مصنوعی ادعا می کند که در آینده پیشرو هوش مصنوعی در جهان خواهد بود.

پیروز شدن در رقابت به این معنی نیست که آمریکا باید تولید فناوری های حیاتی را کنترل کند، بلکه باید بتواند در این عرصه با چین رقابت کند. آمریکا باید در بستر های فناورانه و کنترل زیر ساخت های دیجیتال جهانی تسلط پیدا کند و بتواند فناوری زیستی را برای ایمنی و معیشت شهروندان خود و انرژی های جدید بکار گیرد. اگر آمریکا نتواند برای برتری در سه حوزه مذکور برنامه ریزی کند، پیشرفت در فناوری زیستی و قدرت رایانه و اختراعات نسل بعدی در کشورهایی مانند چین اتفاق خواهد افتاد که فراتر از رقابت نظامی است.

چین سال ۲۰۲۵ را به عنوان سال سلطه بر تولید فناوری های نوظهور هدف گذاری کرده است. این کشور همچنین ادعا می کند تا سال ۲۰۳۰ هدایت جریان هوش مصنوعی در جهان را تحت کنترل خواهد گرفت. این اهداف همزمان با توسعه و افزایش حضور و نفوذ این کشور در بستر شبکه های اجتماعی است.

تحلیل گران بادر نظر گرفتن این موارد و نیز رشد اقتصادی چین، بازه زمانی ۲۰۲۵ الی ۲۰۳۰ را دوره بسیا مهمی برای "ژئو پولتیک" جهانی و امنیت کشورهای رقیب چین به ویژه آمریکا ارزیابی کرده اند.

فناوری های مخرب نوظهور دفاعی

فناوری های مخرب نوظهور EDT= Emergent Destructive Technologies می توانند صحنه جنگ های آینده را متحول کنند. برابر گزارش مرکز تحقیقات پارلمان اتحادیه اروپا، با توجه به اهمیت فناوری های مخرب نوظهور (EDT)، بودجه قابل توجهی به تحقیق و توسعه در این زمینه اختصاص داده شده است. با این حال همگام شدن اتحادیه اروپا با آمریکا، چین و روسیه یک چالش بزرگ برای آن اتحادیه محسوب می شود. مقرارت صندوق دفاعی اروپا (EDA)، فناوری مخرب دفاعی را یک فناوری پیشرفته یا کاملاً جدید تعریف نموده که یک تغییر اساسی در مفهوم "پارادایم" دفاعی ایجاد می کند.

سازمان علم و فناوری "ناتو" فناوری های مخرب نوظهور را اینگونه تعریف می کند:

"فناوری ها یا اکتشافات علمی که تاثیر عمده و انقلابی بر روی عملکردهای دفاعی، امنیتی یا سازمانی داشته باشند".

آژانس دفاعی اروپا (EDA) تاکنون شش فناوری مخرب نوظهور را به شرح ذیل دسته بندی کرده است:

۱- فناوری های مبتنی بر "کوانتوم".

۲- هوش مصنوعی (AI).

۳- "روباتیک" و سامانه های تسلیحاتی خودمختار.

۴- تجزیه و تحلیل داده های بزرگ.

۵- تسلیحات "هایپرسونیک" و فناوری های فضایی.

۶- مواد پیشرفته جدید.

آمریکا سلاح های هدایت کننده انرژی و "بایوتکنولوژی" را نیز به این شش فناوری مخرب اضافه نموده است. فناوریهای مخرب نوظهور برای اهداف نظامی در سطح جهانی، بویژه در چین، روسیه و آمریکا در حال توسعه هستند این موضوع به یک مسابقه تسلیحاتی تبدیل شده و نگرانی های مهمی را ایجاد کرده است.

در قیاس با قدرت های بزرگ جهانی اتحادیه اروپا راه طولانی برای دستیابی به نوآوری های دفاعی پیش رو دارد. جدیدترین داده های آژانس دفاع اروپا (EDA) نشان می دهد که در سال ۲۰۲۰، کشورهای عضو اتحادیه اروپا تنها ۲/۵ میلیارد یورو برای تحقیق و فناوری (R&T) هزینه کرده اند که تنها ۱/۲ درصد از کل هزینه های دفاعی اروپا را تشکیل می دهد. این در حالی است که سازمان دائمی همکاری های اروپا (PESCO)، کشورهای عضو اتحادیه اروپا را متعهد به تامین و افزایش ۲ درصدی هزینه های دفاعی نموده است.

آمریکا حداقل ۱۴ میلیارد دلار، یعنی ۲ درصد از کل بودجه دفاعی آن کشور را برای تحقیق و نوآوری (R&I) هزینه کرده است. آژانس پروژه های تحقیقاتی دفاعی آمریکا (DARPA) که مسئولیت نوآوری های دفاعی را برعهده دارد، فقط در سال ۲۰۲۱ بودجه ای معادل با ۳/۵ میلیارد دلار را دریافت نموده است.

بدست آوردن اطلاعات مربوط به بودجه های نظامی در چین دشوار است. اما گزارش وزارت دفاع آمریکا در مورد تحولات نظامی چین نشان می دهد که این کشور به دنبال تسلط بر فناوری های مخرب نوظهور، از جمله هوش مصنوعی، فناوری های "کوانتومی" و سامانه تسلیحاتی "هایپرسونیک" است. به عنوان مثال: چین هم اکنون دارای موشک های کروز "هایپرسونیک" HCM و "گلایدهایپرسونیک" HGM عملیاتی است.

بدست آوردن اطلاعات مربوط به بودجه های نظامی در مورد روسیه هم مشکل است. اگرچه روسیه اهمیت زیادی برای توسعه فناوری های مخرب نوظهور قائل است اما بعید به نظر نمی رسد بتواند بازیگران اصلی توسعه فناوری های مخرب نوظهور را به چالش بکشد زیرا روسیه تحت تاثیر پیامدهای تحریم بویژه در بخش فناوری های جدید است.

در عین حال روسیه نیز دارای موشک های کروز "هایپرسونیک" HCM و "گلایدهایپرسونیک" HGM عملیاتی است. گزارش شده که روسیه برای اولین بار در جنگ اوکراین از یک موشک هایپرسونیک به نام Kinzhal استفاده کرده است. اگر چه این موشک از نظر فنی مشابه موشک های کروز "هایپرسونیک" HCM و "گلایدهایپرسونیک" HGM نیست اما چالش های دفاعی مشابهی را ایجاد می کند.

آمریکا چندین برنامه تسلیحات "هایپرسونیک" را در دستور کار خود دارد اما بعید است تا قبل از سال ۲۰۲۳ عملیاتی شوند. در اتحادیه اروپا نیز تنها فرانسه تلاش و سرمایه گذاری قابل توجهی در توسعه سلاح های "هایپرسونیک" تهاجمی انجام داده است.

علاوه بر آمریکا، چین، فرانسه و روسیه، هند نیز توجه خاصی به توسعه این فناوری از خود نشان داده است. رهبران اتحادیه اروپا در "ورشو" در مارس ۲۰۲۱ متعهد به افزایش قابل ملاحظه بودجه های دفاعی، از جمله سرمایه گذاری در فناوریها و نوآوری های حیاتی نو ظهور برای، تقویت هم افزایی فضایی، نوآوری و تحقیقات غیر نظامی و دفاعی شدند. اتحادیه اروپا در سال های اخیر فعالیت های متعددی را در این زمینه آغاز کرده است.

صندوق دفاعی اروپا (EDF):

این صندوق ۴ تا ۸ درصد از بودجه سالانه خود را به فناوری های مخرب نو ظهور اختصاص می دهد به عنوان مثال: در فراخوان فناوری های مخرب نو ظهور (EDF 2021) برای توسعه دستگاه سنجش سه بعدی الکترونیکی، بیش از ۵ درصد از بودجه به پروژه مذکور اختصاص یافت. در فراخوان بعدی (EDF 2022)، ۴۰ میلیون یورو، برابر با ۴/۳ درصد بودجه تخصیصی برای تحقیقات و ۵۴۱ میلیون یورو دیگر برای تحقیق و توسعه شرکت های کوچک و متوسط در نظر گرفته شد.

ترویج هم افزایی تحقیق و نوآوری (R&I) غیر نظامی و دفاعی:

برخلاف بسیاری از نوآوری های انقلابی مانداینترنت، که در ابتدا توسط ارتش توسعه یافت، نوآوری در حوزه فناوری های مخرب نوظهور عمدتاً در بخش غیرنظامی متمرکز است. برنامه اقدام "کمسیون" اروپا به دنبال افزایش بودجه های تکمیلی برای برنامه های دفاعی مانند Horizon Europe و صندوق دفاعی اروپا (EDF) است تا از ظرفیت فناوری های مذکور در کاربری های غیر نظامی فضایی و دفاعی استفاده کند.

طرح های نوآوری دفاعی اتحادیه اروپا:

این طرح با یک بسته مالی ۲ میلیارد یورویی شامل ۱/۴۶ میلیارد یورو از پروژه های صندوق دفاعی اروپا (EDF)، ۹۰ میلیون یورو از کمک های مالی مشترک کشورهای عضو و ۴۰۰ تا ۵۰۰ میلیون یورو از سایر منابع، برای نوآوری و کار آفرینی در زمینه فناوری های مذکور تعیین کرده است.

سازمان دائمی همکاری های اروپا (PESCO):

سازمان دائمی همکاری های اروپا (PESCO) که در سال ۲۰۱۷ برای تعمیق همکاری دفاعی بین ۲۶ کشور عضو اتحادیه اروپا تاسیس شد، در زمینه توسعه فناوری های مخرب نوظهور فعالیت می کند. این ساختار قبلاً توسط کشورهای عضو برای شروع توسعه فناوری های مربوط به پروژه دفاع موشکی "هایپرسونیک" موسوم به Twister و Euro drone اقدام مشابهی انجام داده بود.

آژانس دفاعی اروپا (EDA):

آژانس دفاعی اروپا (EDA)، از زمان تاسیس در سال ۲۰۰۴ در زمینه نوآوری های دفاعی اروپا فعالیت می کند و فناوری های مخرب نوظهور یکی از اصلی ترین فعالیت های تحقیقاتی و فناوری آن است. آژانس دفاعی اروپا قبلاً پروژه هایی مثل پروژه Euro Swarm را ارایه کرده است که استفاده موثر از پهپادهای گروهی Swarm، از فعالیت های این آژانس به شمار می رود.

مرکز نوآوری های دفاعی اروپا (HEDI):

مرکز نوآوری های دفاعی اروپا (HEDI) در سال ۲۰۲۲ راه اندازی شد تا فعالیتهای نوآورانه آژانس را تقویت کند و فعالیت های جدید را بطور مشترک با کشورهای عضو تسریع نماید.

پارلمان اروپا خواستار توجه ویژه به تاثیر فناوری های نوظهور، بویژه هوش مصنوعی برای استفاده احتمالی آنها در حوزه امنیت شده و ضمن تاکید بر اهمیت همکاری فرا "آتلانتیکی" در مورد فناوری های مخرب نوظهور از اتحادیه اروپا و "ناتو" می خواهد تا تلاش های مشترک برای دست یابی و حفظ رهبری فناورانه جهانی در حوزه نظامی نیز افزایش یابد. پارلمان اروپا همچنین خواستار تلاش های جهانی برای ایجاد یک چارچوب نظارتی جامع برای راهبری سلاح های مجهز به هوش مصنوعی و تنظیم یک سند الزام آور قانونی برای ممنوعیت سامانه های تسلیحاتی کاملاً خود مختار است.

کاربرد هوش مصنوعی برای شناسایی اهداف توسط تانک جدید ارتش آمریکا

شرکت "جنرال داینامیکس" به تازگی نمونه اولیه نسل بعدی تانک های خود از خانواده تانک "آبرامز" را به نمایش گذاشته است. بازطراحی این تانک با نام Abrams x بزرگترین باز طراحی و ارتقاء فناوری تانک های نظامی آمریکا از زمان جنگ سرد تاکنون است که ضمن دارا بودن ویژگی های متعارف، تغییرات مهمی در طراحی و کاهش هزینه های عملیاتی نیز داشته است. این تانک از یک موتور "هیبریدی" استفاده می کند که سبک تر و بسیار کم مصرف تر از تانک های "آبرامز" فعلی است. در باز طراحی جدید، تعداد خدمه این تانک کاهش یافته و به جای آن سامانه های مبتنی بر هوش مصنوعی، شناسایی دشمن را به عهده گرفته اند.

وزن این تانک بسیار کمتر از مدل های فعلی است. موتور "هیبریدی" آن سوخت کمتری مصرف نموده و طراحی آن به گونه ای است که سربازان به جای استقرار در برجک، در بدنه تانک استقرار یابند. همانگونه که اشاره شد تعداد خدمه این تانک جدید، کاهش یافته و احتمالاً سه خدمه خواهد داشت و برای محافظت در برابر بمب هایی که توسط هواپیماهای بدون سرنشین پرتاب می شود از زره پیشرفته تری بهره برداری می کند.

ارتقاء نرم افزارها، از جمله بهینه سازی های مهم صورت گرفته بر روی این تانک محسوب می گردد. سامانه هوش مصنوعی بکار گرفته شده در این تانک، وظیفه تشخیص خطرات از فواصل دور را بر عهده دارد. این نرم افزار می تواند به خدمه هشدار دهد که تانک های دشمن در چه فواصلی مستقر هستند و به صورت بالقوه چند درصد احتمال آسیب رسانی دارند. این تانک همچنین می تواند با هواپیماهای بدون سرنشین ارتباط برقرار کرده و خطرات پیش رو را شناسایی کند و با استفاده از هوش مصنوعی در صورت وجود تهدید نسبت به اولویت بندی تهدیدات اقدام نماید. ارتش آمریکا در تلاش برای ارتقاء قابلیت های عملیاتی تانک های خود و استفاده از هوش مصنوعی، به شکل مطلوب تری برای این تجهیزات می باشد.

رمز گذاری کوانتومی ماهواره برای تقویت استقلال اروپا

آژانس فضایی اروپا (ESA)، کمیسیون اروپا و برخی از شرکت های فضایی در اروپا در نظر دارند به منظور ایجاد سامانه ارتباطی ماهواره ای بسیار ایمن برای اتحادیه اروپا با یکدیگر همکاری نمایند.

ماهواره Eagle-1 اولین سامانه توزیع کلید "کوانتومی" فضا پایه در اروپا خواهد بود که با مشارکت ESA و شرکت SES (کنسرسیوم متشکل از ۲۰ شرکت اروپایی که مقر آن در لوکزامبورگ است) و با حمایت کمیسیون اروپا، توسعه می یابد. این ماهواره راه را برای ایجاد یک شبکه فوق امن که برای ایمن نگاهداشتن اطلاعات، که بر قوانین مکانیک "کوانتومی" متکی است هموار می کند و استقلال اروپا در امنیت سایبری و ارتباطات را بطور قابل توجهی افزایش می دهد. ماهواره Eagle-1 از فناوری توزیع کلید "کوانتومی" که از اصول مکانیک "کوانتوم" برای توزیع کلید های رمز گذاری است استفاده می کند به گونه ای که هر گونه تلاش برای استراق سمع بلافاصله شناسایی می شود. به این منظور این سامانه براساس فناوری های کلیدی توسعه یافته تحت برنامه Skylight ESA با هدف اعتبارسنجی اجزای حیاتی عرضه شده در اتحادیه اروپا ساخته می شود.

فناوری های توزیع کلید "کوانتومی" از مدار پایین زمین تا سطح زمین را پوشش می دهد و داده های ارزشمندی را برای توسعه و استقرار زیرساخت های ارتباطی "کوانتومی" اروپا (Euro QCI) ارایه می کند که در سامانه اتصال امن اروپا یکپارچه خواهد شد. این موضوع به اتحادیه اروپا اجازه می دهد تا برای یک شبکه ارتباطی "کوانتومی" ایمن و مستقل آماده شود.

این سامانه در ابتدا از یک ترمینال زمینی نوری ارتقاء یافته از مرکز هوافضای آلمان (DLR) در کناریک ترمینال زمینی نوری جدید که توسط گروهی از متخصصان هلندی ساخته خواهد شد، استفاده خواهد کرد. ماهواره Eagle-1 متعلق به شرکت ایتالیایی Siatel، محموله ای با کلید "کوانتومی" ساخت شرکت Tesat Spacecom آلمان را همراه خواهد داشت و توسط شرکت SES اداره خواهد شد. کشورهای اتریش، بلژیک، جمهوری چک، ایتالیا و سوئیس نیز در این پروژه همکاری دارند. قرار است ماهواره Eagle-1 در سال ۲۰۲۴ پرتاب شود و پس از سه سال آزمایشهای مداری آن با پشتیبانی کمیسیون اروپا انجام شود. نوآوری فضایی در اروپا هم از منظر فناوری و هم از نظر تجاری سازی شتاب بیشتری پیدا کرده است که در حوزه فناوری و ایمن سازی اطلاعات جایگاه ویژه ای دارد.