۵۵

موسسه اطلاع رسانی امور سایبری

Cyberban World News Agency • فصل نامه تابستان ۱۴۰۲

دیپلماسی موفق سایبری دولت سیزدهم

کمپ منافقین در آلبانی، مغلوب دیپلماسی سایبری ایران

- مصاحبه اختصاصی سایبربان درمورد عدم رجیستری آیفون۱۴ و بازی واقعیت مجازی مخاطرات
- هوش مصنوعی همزادی شیطانی برای اختلال در طبیعت انسان
- گروه انتقام جویان سایبری و حملات به رژیم صهیونیستی
- بررسی نکات سایبری در نشست رهبران ناتو
- گسترش وب تاریک و ارزش نظارت بر آن
- استقلال، پرسپولیس و جرائم سایبری
- نمایشگاه هوایی پاریس



سخـــن ســردبیر

همراهان گرانقدر پروردگار بلند مرتبه را سپاس بی نهایت که بار دیگر توفیق و فرصتی دوباره دست داد تا به بهانه انتشار مجدد نشریه با شما خوانندگان گرانمایه و فرهیخته به گفتگو بپردازم. پس از چندین سال با پنجاه و پنجمین شماره از مجلات سایبربان در سال دهم همراه نگاه پر مهر شما مخاطبین عزیز هستیم و صادقانه میگویم، تداوم انتشار نشریه بدون مشارکت شما امکان پذیر نخواهد بود.

این ویژه نامه می کوشد تا به بررسی برخی از رویدادهای فصلی که گذشت بپردازد و مهم ترین آن ها را به پیشگاه مخاطبین محترم تقدیم کند.

در عرصه جنگ سایبری بحران رژیم صهیونیستی در تامین امنیت سایبری بسیار پیچیده تر و حساس تر گشته است. انتقام جویان سایبری جدیدترین گروه مهاجمی است که حملات گسترده ای را از چندین سال قبل تا به حال بر عهده گرفته و این روزها خبرساز میدان حملات سایبری به رژیم شده است.

در عرصه بین الملل همچنان پرونده جنگ روسیه و اوکراین سرشار از شگفتانه های جنگ سایبری می باشد و جهان نظاره گر این زوایای جنگی است. در این میان نشست رهبران ناتو در لیتوانی و نکات سایبری مطرح شده از اهمیت ویژه ای برخوردار است.

همانطور که می دانید ایران از ابتدای دولت آقای رئیسی به طور جدی تری درگیر حملات سایبری شده است، حملاتی که با پرچم های مشخصی صورت گرفت و در آن میان، منافقین از همه بیشتر نقش آفرینی کردند. بدون شک دیپلماسی سایبری موفق دولت سیزدهم در ماجرای کمپ اشرف آلبانی به عنوان اقدامی بی سابقه در نظام جمهوری اسلامی خواهد ماند.

در عرصه شبکه های اجتماعی، همچنان حاکمیت سایبری به معنای واقعی اتفاق نیفتاده است و حاشیه های این ماجرا را پایانی نیست، باید دید که چگونه در این میان حوزه ورزش به ویژه فوتبال هنوز در میان پلتفرم های غیر قانونی بی محابا جولان می دهد و به هیچ مقام و مرجعی هم پاسخگو نیست؟

در عرصه فناوری اتفاق بزرگی در پاریس افتاد که در میان صفحات اخبار کم رنگ تر به آن پرداخته شد. نمایشگاه هوایی پاریس و رونمایی از دستاوردهای جدید صنعت هوا و فضا خبر از اتفاقات جدیدی در این حوزه برای آینده دارد. بررسی شرکت های حاضر در این رویداد و عقد قراردادها و همکاری ها، بُعد دیگری از فناوری را در پاریس به نمایش گذاشته است.

چندین حوزه دیگر از قبیل امنیت سایبر، هوش مصنوعی، هنر و سایبر، بدافزار و باج افزار، مصاحبه های اختصاصی، فناوری های نظامی، وب تاریک و معرفی آثار سایبری در این شماره از مجله با کوشش همکارانم برای شما مخاطبان گرامی به رشته تحریر درآمده است.

در آخر از بابت تمامی کم و کاستی ها صمیمانه پوزش می‌طلبم و امید آن دارم تا این موسسه با ایفای نقش رسانه ای خود در حوزه سایبر و با اطلاع رسانی های شایسته ، آگاهی بخش مردم عزیز کشورمان باشد و شما مخاطب فرهیخته را خشنود سازد.

سید احمد موسوی

ماه نامه خبری-تحلیل سایبربان (ویژه نامه فصل تابستان)

سال دهم ، شماره ۵۵ ، تیر- مرداد - شهریور ۱۴۰۲

تهیه و تنظیم و نشر : موسسه اطلاع رسانی سایبربان

تمامی حقوق مادی و معنوی این ماهنامه محفوظ و مربوط به موسسه اطلاع رسانی سایبربان می باشد.

انتشار به صورت محدود

سایبربان

مؤسسه اطلاع رسانی امور سایبری

آنان که با واژه «Cyber» آشنا هستند، می‌دانند که این رزم‌گاه نوین، اهرمی برای اجرای سیاست‌های حکومت‌ها، در بخش‌های گوناگون است. شایان یادآوری، آن که مؤسسه اطلاع‌رسانی سایبربان، یکی از مراکز تخصصی است که با رصد رویدادهای رایانیکی و واکاوی آن‌ها، به ارتقای سطح امنیت در میهنمان، کمک می‌کند.

@cyberbannews_ir
@cyberbannews_ir
Cyberbanmedia
@cyberbannews_ir
CyberbanNews
www.cyberbannews.com
@cyberbanmedia@gmail.com

با سایبربان

همراه باشید...

@cyberbannews_ir

موسسه اطلاع رسانی امورسایبری
cyberban News Agency
مرجع تخصصی امور سایبری در ایران
www.cyberbannews.com

فهرست



۲.حمله گروه هکری انتقام جویان به شبکه راه آهن رژیم صهیونیستی
۴. افشای اطلاعات زیر ساخت های مهم رژیم صهیونیستی
۶. ضعف رژیم صهیونیستی در تامین امنیت سایبری زیر ساخت ها

بین الملل و سایبر

۸ . نشست رهبران ناتو در لیتوانی و بررسی نبرد اوکراین و روسیه از بعد سایبری



۱۰. کمپ منافقین مغلوب دیپلماسی موفق سایبری دولت سیزدهم
۱۲.ردپای روسیه در تنش سایبری سال گذشته میان ایران و آلبانی
۱۴. حمله سایبری به بنیاد شهید

سایبر ورزش

۱۶. استقلال و پرسپولیس و جرایم سایبری



۱۸. نظارت پلتفرم های آنلاین چین بر اطلاعات کاربران
۱۹ .نقض حقوق کاربر در پیام رسان بله



۲۰. مصاحبه اختصاصی با احمد رضا امینی سازنده بازی واقعیت مجازی مخاطرات
۲۴. پشت پرده ماجرای ممنوعیت رجیستری آیفون ۱۴ و بازار اپل در ایران

سایبر اینفوگرافی

۲۸. ذخیره داده ها بر DNA



۳۰.نمایشگاه هوایی پاریس در سال۲۰۲۳
۳۶.پنج نوآوری برتر فناوری نظامی اوکراین

هوش مصنوعی

۴۰. هوش مصنوعی همزادی شیطانی برای اختلال در طبیعت انسان



۴۲. چگونه از گوشی خود در برابر بد افزار ها محافظت کنیم
۴۴. اصابت ترکش یک کمپین بد افزاری جدید به وزارت دفاع آمریکا
۴۶. سرقت داده از ضربات کلید کیبورد با دقت ۹۵ درصد
۴۸. با بدافزار جدید و کم نظیر بورات آشنا شوید

وب تاریک

۵۰.گسترش وب تاریک و ارزش نظارت بر آن

هنر و سایبر

۵۲. معرفی و بررسی کتاب هنر قانون سایبری و جرایم سایبری
۵۴. سایبر سینما ، هوش مصنوعی و نگاهی به فیلم سینمایی ناشنیده

حمله گروه انتقام جویان سایبری به شبکه راه‌آهن رژیم صهیونیستی

رسانه‌های اسرائیلی اعلام کردند که گروه هکری انتقام جویان سایبری شبکه راه آهن رژیم صهیونیستی را هدف قرار داد.

تروریسم سایبری



به گزارش کارگروه حملات سایبری سایبربان؛ رسانه‌های اسرائیلی اعلام کردند که شبکه راه‌آهن رژیم صهیونیستی هدف حمله سایبری قرار گرفت.

گروه هکری انتقام جویان سایبری (Cyber Avengers) اطلاعاتی را فاش کرده که نشان می‌دهد زیرساخت‌های برق سیستم راه‌آهن اسرائیل را هدف قرار داده است. شرکت راه‌آهن رژیم صهیونیستی اعلام کرد که در حال فراهم کردن اتوبوس به عنوان جایگزین است، اما افرادی که قصد تردد به محل کار یا بالعکس را دارند، باید از سایر وسایل حمل و نقل استفاده کنند. هفته گذشته نیز خدمات ریلی در مرکز سرزمین‌های اشغالی به دلیل مشکل فنی، موقتاً به حالت تعلیق درآمد. از سال ۲۰۲۰، گروه هکری انتقام جویان سایبری ، حملات سایبری متعددی را علیه سیستم‌های راه‌آهن اسرائیل انجام داده‌اند.

این گروه هشدار داد که اگر رژیم اشغالگر اسرائیل به جنایات خود ادامه دهد، ضربات هولناکی به زیرساخت‌هایش وارد خواهد کرد. شایان ذکر است که انتقام جویان سایبری چند وقت قبل مسئولیت حمله‌ای را بر عهده گرفته بود که زیرساخت‌های بازان (Bazan)، بزرگ‌ترین پالایشگاه تولیدکننده بنزین در اراضی اشغالی را هدف قرار داده بود. در ماه‌های اخیر، زیرساخت‌ها و وب‌سایت‌های رژیم صهیونیستی مورد حملات سایبری گسترده ای از سوی چندین گروه هکری قرار گرفتند. در اواسط ماه می سال جاری، رسانه‌های اسرائیلی گزارش دادند که وب‌سایت فرودگاه بن‌گوریون در تل آویو به دلیل یک حمله سایبری از کار افتاده است. وب‌سایت خبری اسرائیلی راتر نت (Rotter Net) نیز به دلیل حمله سایبری گروه هکری انانیموس سودان (Anonymous Sudan) آفلاین شد، در حالیکه سایر حملات برنامه سیستم هشدار اضطراری اسرائیل که به عنوان هشدار قرمز نیز شناخته می‌شود را هدف قرار داد.

رسانه‌ها همچنین در اواسط آوریل امسال گزارش دادند که بیش از ۶۰ وب‌سایت اسرائیلی تنها در چند روز تحت موج سنگین حملات سایبری قرار گرفتند. این اهداف شامل سایت‌های دولتی رژیم اشغالگر، روزنامه‌های اصلی و خدمات عمومی بود که برخی هک‌ها منجر به تصرف پایگاه‌های اطلاعاتی شد. در نتیجه، رونن بار (Ronen Bar)، رئیس آژانس امنیت جاسوسی اسرائیل موسوم به شین‌بت (Shin Bet)، در اواخر ژوئن سال جاری تأیید کرد که تل آویو در حال توسعه سیستم گنبد آهنین سایبری جهانی با همکاری تعدادی از کشورها برای شناسایی تهدیدات سایبری با استفاده از هوش مصنوعی (AI) است.



مبارزه با تروریسم سایبری

افشای اطلاعات زیرساخت‌های مهم رژیم صهیونیستی توسط گروه هکری انتقامجویان سایبری

گروه هکری انتقامجویان سایبری در کانال تلگرامی خود تصاویری از حملات سایبری علیه زیرساخت‌های رژیم صهیونیستی را در ماه اوت منتشر کرد.

به گزارش کارگروه حملات سایبری سایبربان؛ گروه هکری انتقامجویان سایبری (Avengers Group) از برخی حملات سایبری علیه زیرساخت‌های مهم رژیم صهیونیستی رونمایی کرد؛ این گروه هکری در کانال تلگرامی خود تصاویری از حملات هکری را منتشر کرد و اظهار داشت که پشت بسیاری از حملات سایبری علیه رژیم غاصب بوده است.

انتقام‌جویان سایبری که سال‌ها رفتار و ادعاهای رژیم صهیونیستی را رصد می‌کند، مصمم است که هیچ جنایت و حرکتی را بی‌پاسخ نگذارد.

در پیام این گروه هکری آمده است

«ما هر حمله شما را که منکر آن می‌شوید، به تمام دنیا ثابت خواهیم کرد. مطمئناً شما ما را بهتر از هرکسی می شناسید... ما به متحدان و حامیان اسرائیل در سراسر جهان هشدار می دهیم، هرگونه حمایت و همبستگی در جنایات این رژیم از جمله آتش زدن قرآن که مصداق خیانت به مسلمانان جهان است و عواقب دردناکی در پی خواهد داشت. بازگشت ما برای شما بسیار دردناک‌تر از قبل خواهد بود...»

گروه بازان ، بزرگ‌ترین شرکت پتروشیمی رژیم صهیونیستی است که انحصار بخش عمده‌ای از صادرات صنایع شیمیایی رژیم صهیونیستی به کشورهای اروپایی و آمریکا را در دست دارد؛ گروه هکری انتقام‌جویان سایبری مسئولیت حمله و ایجاد نقص در سیستم‌های این پالایشگاه را در سال‌های مختلف برعهده گرفت و تصاویری از نقص در سیستم‌های شرکت را در کانال خود منتشر کرد.

در میان تصاویر منتشر شده، تصاویری از تلاش آتش‌نشانان برای خاموش کردن آتش‌سوزی ۳۰ آوریل ۲۰۲۱ در پالایشگاه نفت بازان در خلیج حیفا دیده می‌شود. همچنین نقص در مجتمع بازان و نبرد نسخه‌ها بین اتحادیه شهرها و بازان در ۲۷ اوت همان سال، ایجاد نقص عملکردی در یکی از تأسیسات بازان و متصاعد شدن دود سیاه آلاینده به خلیج حیفا که نشان دهنده میزان بالای بنزن سرطان‌زا نیز بود و ساکنان این خلیج را آلوده کرد در ۱۵ ژوئن سال ۲۰۲۲، نقص در سیستم تصفیه تأسیسات کراکر کاتالیزوری پالایشگاه گروه بازان در ۲۸ نوامبر ۲۰۲۲، سوختن ترانسفورماتور برق در کارمل الفین حیفا در ۶ دسامبر ۲۰۲۲ و نقص در پالایشگاه‌ها و ایجاد آتش‌سوزی در ۲۲ فوریه ۲۰۲۳ از جمله حملات سایبری این گروه هکری بوده است.

ویدئویی هم پخش شد که نقص عملکردی در یکی از تأسیسات بازان و متصاعد شدن دود سیاه آلاینده به خلیج حیفا که نشان دهنده میزان بالای بنزن سرطان‌زا نیز بود و ساکنان این خلیج را آلوده کرد در ۱۵ ژوئن سال ۲۰۲۲ را نشان می‌دهد.

انتقام جویان که ۳۰ ژوئیه اعلام کرده بودند که به زودی شگفتانه و افشاگری های تازه ای را منتشر خواهند کرد، درست طبق ساعت اعلام شده یعنی ۶:۳۰ با سیستم سانسور بین المللی رژیم صهیونیستی مواجه شدند و پس از نشر جمله (HELLO Checkpoint) کانال تلگرام و اکانت توئیتر این گروه هکری کاملا از دسترس خارج شده است.

برخی هک‌های گروه انتقام جویان سایبری به شرح زیر است :

- نقص عملکرد در یکی از تأسیسات بازان و متصاعد شدن دود سیاه آلاینده به خلیج حیفا که نشان دهنده میزان بالای بنزن سرطان‌زا نیز بود و ساکنان این خلیج را آلوده کرد در ۱۵ ژوئن سال ۲۰۲۲
- نقص در سیستم تصفیه تأسیسات کراکر کاتالیزوری پالایشگاه گروه بازان در ۲۸ نوامبر ۲۰۲۲
- نقص در پالایشگاه‌ها و ایجاد آتش‌سوزی در ۲۲ فوریه ۲۰۲۳
- سوختن ترانسفورماتور برق در کارمل الفین حیفا در ۶ دسامبر ۲۰۲۲
- اختلال در وب‌سایت‌های گروه بازان
- حمله سایبری و انفجار ۲۰ مخزن گاز در اسرائیل
- حمله سایبری به شبکه راه‌آهن رژیم صهیونیستی



AVENJER.....
CUBER

ضعف رژیم صهیونیستی در تامین امنیت سایبری زیر ساخت ها



■ **خبرگزاری اورشلیم پست با انتشار گزارشی نسبت به وضعیت زیرساخت‌های حیاتی رژیم صهیونیستی انتقاد کرد؛**

این رسانه عنوان کرد که چرا این بخش‌ها در برابر حملات سایبری آسیب‌پذیر هستند؟ درواقع این رسانه اعتقاد دارد تا زمانی که مقررات جدیدی درباره وضعیت سایبری اتخاذ نشود، مشکلات ادامه خواهند داشت.

■ یکی از این موارد، **حمله سایبری علیه مرکز پزشکی مایانئی هایشوا بود**؛ این مورد از موضوعاتی است که می‌تواند بخش بهداشت را تحت تأثیر خود قرار دهد. از جهاتی این حمله یک تهدید امنیت ملی به شمار می‌رود و باید به این نکته توجه کرد که **رژیم صهیونیستی و سرزمین های اشغالی بسیار کوچک است و مراکز درمانی بسیار اندکی دارد.** در ماه گذشته گذشته نیز بیش از **۱۰۰ مرکز پزشکی در آمریکا موردحمله سایبری گسترده قرار گرفتند**، البته این موضوع جدیدی نبود؛ در سال ۲۰۲۱ نیز حمله مشابهی در آمریکا و دیگر کشورهای جهان رخ داد. با تمام این اوصاف، تقریباً همه کارشناسان سایبری موافق هستند که بخش پزشکی رژیم صهیونیستی مثل همیشه آسیب‌پذیر است؛این رسانه عنوان کرد که واقعاً چرا بیمارستان‌های ما در برابر حملات سایبری آسیب‌پذیر هستند؟ چرا ما خود را برای مقابله آماده نکرده‌ایم؟

■ بیشتر مردم این حملات را تا زمانی که منجر به مرگ بیماران نشود، نادیده می‌گیرند؛ اما موضوع موردبحث این است که حتی خود کارشناسان هم نمی‌توانند درباره چگونگی حل این مشکل به توافق برسند. درباره این موضوعات دیکلا ورد (Dikla Vered)، معاون مدیرعامل شرکت «Experis» ، گفت: «کشور هنوز از حمله به مرکز پزشکی هیلل یافه درس نگرفته است. واقعاً عجیب است که اسرائیل هنوز بخش بهداشت را در فهرست زیرساخت‌های حیاتی خود قرار نداده است.»

■ **ییگال اونا (Yigal Unna)، رئیس سابق اداره ملی سایبر** (از سال ۲۰۱۸ الی ۲۰۲۲) اعتقاد داشت که باید دسترسی‌های دولت افزایش‌یافته و بخش‌هایی را به زیرساخت‌های حیاتی اضافه کرد؛ درواقع او اعتقاد داشت که رژیم صهیونیستی باید نوعی قانون سایبری برای افزایش تعادل و تعامل بین بخش خصوصی و دولتی تصویب کند. او و رئیس فعلی اداره ملی سایبر دیدگاه‌های بسیار متفاوتی در این زمینه دارند. بنیامین نتانیاهو، پیش از این طی نشستی با وزرای کلیدی و رهبران سایبری به آن‌ها دستور داده تا برای دفاع از زیرساخت های حیاتی، فعالیت‌هایی را پیگیری کرده و مقررات را اجرا کنند. این دستور نتانیاهو، ایراداتی داشت؛ ازجمله آن‌که برای اجرای آن زمانی تعیین نشده و با توجه به اینکه تقریباً از آن زمان کنست تمرکز خود را بر لایحه قضایی گذاشته، به نظر می‌رسد در ماه های آتی نیز هیچ‌گونه تغییر و تحولی در این زمینه وجود نداشته باشد. باید به این موضوع توجه داشت، تا زمانی که اسرائیل درباره مقررات جدید سایبری تصمیم‌گیری نکند، مشکلات وجود خواهند داشت. نهایتاً، ایران و سایر کشورهایی که به دنبال آسیب رساندن به رژیم صهیونیستی هستند، همچنان فرصت‌هایی برای آسیب رساندن به امنیت ملی را خواهند داشت که این موضوع باید موردتوجه بیشتری قرار بگیرد.

نشست رهبران ناتو در لیتوانی و نکات سایبری



شهر ویلنیوس، پایتخت لیتوانی، در ماهای گذشته میزبان نشست ناتو بود. در این نشست روی مسئله نبرد اوکراین و روسیه، تمرکز شد. در این گزارش، رهبران ناتون اعلام کردند:

■ ما همچنان با تهدیدهای سایبری، فضایی، ترکیبی و سایر تهدیدهای نامتقارن و استفاده مخرب از فناوری های نوظهور و ویران ساز مواجه هستیم.

■ روسیه اقدامات ترکیبی خود را علیه متحدان و شرکای ناتو ازجمله از طریق نائبان خود تشدید کرده است. این موضوع شامل دخالت در فرآیندهای دموکراتیک، اجبار سیاسی و اقتصادی (مانند تحریم)، کمپین‌های گسترده اطلاعات نادرست (disinformation)، فعالیت های مخرب سایبری، و فعالیت‌های غیرقانونی و مخرب سرویس‌های اطلاعاتی روسیه است.

■ عملیات مخرب ترکیبی و سایبری چین و لفاظی های تقابلی و اطلاعات نادرست آن، متحدان ناتو و ناتو را هدف قرار داده و به امنیت آن آسیب می رساند. چین به دنبال کنترل بخش‌های کلیدی فناوری و صنعتی، زیرساخت‌های حیاتی و موارد استراتژیک و زنجیره‌های تأمین است. چین به دنبال کنترل بخش‌های کلیدی فناورانه و صنعتی، زیرساخت‌های حیاتی و مواد استراتژیک و زنجیره های تأمین است. این کشور از اهرم اقتصادی خود برای ایجاد وابستگی‌های استراتژیک و افزایش نفوذ خود استفاده می‌کند. این کشور تلاش می کند تا نظم بین‌المللی قانون محور، ازجمله در حوزه فضایی، سایبری و دریایی را بر هم بزند.

■ موقعیت بازدارندگی و دفاعی ناتو مبتنی بر ترکیب مناسبی از قابلیت‌های دفاعی هسته ای، متعارف و موشکی است که باقابلیت های فضایی و سایبری تکمیل می‌شود.

■ موافقت کردیم که به کار خود در عملیات چند حوزه ادامه دهیم که توسط تحول دیجیتال ناتو امکان‌پذیر شده است و مزیت نظامی و تکنولوژیکی ما را بیشتر و توانایی ناتو برای عملیات قاطع در سراسر زمین، هوایی، دریایی، فضای سایبری و فضایی را تقویت می‌کند.

■ **فضای سایبری همیشه مورد مناقشه است؛ زیرا بازیگران تهدیدآمیز این فضا، به صورت روزافزون به دنبال بی‌ثبات کردن ناتو با استفاده از فعالیت‌ها و کمپین‌های مخرب سایبری هستند. جنگ روسیه علیه اوکراین نشان داده است که تا چه حد بُعدسایبری از ویژگی‌های درگیری مدرن است.**

■ ما در حال مقابله با تهدیدات سایبری اساسی، مستمر و روزافزون، ازجمله تهدید علیه سیستم های دموکراتیک و زیرساخت‌های حیاتی خود هستیم که بخشی از کارزارهای هیبریدی هستند.

■ ما مصمم هستیم که طیف کاملی از قابلیت ها را به‌منظور بازدارندگی، دفاع و مقابله با طیف کامل تهدیدات سایبری، ازجمله با در نظر گرفتن پاسخ‌های جمعی، به کار بگیریم.

■ مجموعه واحد یا جمعی از فعالیت‌های مخرب سایبری می‌تواند به سطح حمله مسلحانه برسد و ناتو را به استناد ماده ۵ معاهده واشنگتن (Washington Treaty) سوق دهد. همچنان ما متعهد هستیم که مطابق با قوانین بین‌المللی، ازجمله منشور سازمان ملل، حقوق بشردوستانه بین المللی و قوانین بین‌المللی حقوق بشر، عمل کنیم.

■ ما به ترویج فضای سایبری آزاد، باز، صلح آمیز و امن ادامه می‌دهیم و تلاش‌ها را برای تقویت ثبات و کاهش خطر درگیری به‌وسیله پشتیبانی از هنجارهای رفتار مسئولانه در فضای سایبری ادامه می‌دهیم.

■ امروز، ما مفهوم جدیدی را برای افزایش سهم دفاع سایبری در بازدارندگی و موقعیت دفاعی خود تأیید می‌کنیم. این سه سطح دفاع سایبری ناتو (سیاسی، نظامی و فنی) را بیشتر ادغام خواهد کرد. تقویت انعطاف‌پذیری سایبری ما برای ایمن تر کردن اتحاد ناتو و توانایی بهتر برای کاهش خطرات بالقوه خطرات سایبری، کلیدی است.

■ امروز ما تعهد دفاع سایبری (Cyber Defence Pledge) خود را تقویت می کنیم و متعهد به اهداف ملی جدید برای تقویت بیشتر دفاع سایبری ملی خود، ازجمله اولویت زیرساخت‌های حیاتی در هستیم.

■ ما قابلیت جدید پشتیبانی از رویدادهای سایبری مجازی ناتو را برای حمایت از تلاش‌های ملی در پاسخ به فعالیت های مخرب سایبری راه‌اندازی کرده‌ایم.

■ ما بیشتر به دنبال توسعه مشارکت‌های سودمند و مؤثر دوجانبه در صورت لزوم، ازجمله با کشورهای شریک، سازمان‌های بین‌المللی، صنعت و دانشگاه خواهیم بود و تلاش‌های خود را برای تقویت ثبات بین‌المللی در فضای سایبری بیشتر می‌کنیم.

■ اولین کنفرانس جامع دفاع سایبری ناتو را در نوامبر امسال در برلین برگزار خواهیم کرد که تصمیم‌گیرندگان را در سطوح سیاسی، نظامی و فنی گرد هم می‌آورد.

■ ما همچنین در ارتباطات راهبردی به نتایج ملموسی ازجمله مبارزه با اطلاعات نادرست، مقابله با تهدیدات ترکیبی و سایبری، رزمایش، همکاری عملیاتی، قابلیت‌های دفاعی، صنایع و تحقیقات دفاعی، مبارزه با تروریسم و ظرفیت‌سازی دفاعی و امنیتی دست‌یافته‌ایم.

■ ما به تقویت گفت‌وگوهای سیاسی و همکاری عملی خود برای حمایت از اصلاحات، صلح و امنیت منطقه‌ای و مقابله بانفوذ مخرب، ازجمله تهدیدات نادرست، ترکیبی و سایبری که توسط بازیگران دولتی و غیردولتی ایجاد می‌شود، ادامه خواهیم داد.

■ ما از پیشرفت‌های حاصل‌شده در اجرای بسته اساسی ناتو-گرجستان، (Substantial NATO-Georgia Package) ازجمله مدیریت بحران، امنیت سایبری، مهندسی نظامی، ارتباطات امن و همچنین ابتکارات جدید در حوزه های دفاع شیمیایی، بیولوژیکی، رادیولوژیکی و هسته‌ای و امکانات آموزشی استقبال می‌کنیم.

■ ما گفت‌وگو و همکاری خود را برای مقابله با چالش‌های امنیتی مشترک خود، ازجمله در زمینه دفاع سایبری، فناوری و ترکیبی که با تعهد مشترک ما به حمایت از قوانین بین المللی و نظم بین‌المللی مبتنی بر قوانین حمایت می‌شود، تقویت خواهیم کرد.

جمع‌بندی و تحلیل ما :

برخی متحدان ناتو به این موضوع اذعان دارند که در صورت وقوع حمله سایبری، ایجاد اختلال و قطع برق نیروگاه دشمن از طریق سایبری، بسیار مؤثرتر از حملات هوایی به آن کشور خواهد بود، زیرا در بسیاری از مواد حملات سایبری به زیرساخت های حیاتی و شریان‌های اصلی یک کشور فلج کننده بوده و موجب اختلالات گسترده می‌شود. ۲۹ کشور عضو ناتو در پیمانی که در سال ۲۰۱۴ به امضا رساندند، فضای سایبر را در کنار زمین، هوا و دریا، **بعد چهارم دامنه جنگ دانستند. ناتو با نظامی کردن فضای سایبری، قصد دارد کاستی‌های دیگر در بخش‌های نظامی را جبران کرده و خلأهای موجود را با سایبر پوشش دهد. شاید به همین دلیل باشد که ناتو در حال ارائه نظریاتی مبنی بر اعمال ماده ۵ این پیمان (در حوزه دفاع جمعی) در عرصه حملات سایبری است. یکی از دلایل دیگر ناتو برای داشتن دید نظامی به فضای سایبری، تهدیداتی است که از سوی روسیه علیه اروپای شرقی می‌داند.** ناتو برای انجام عملیات سایبری جمعی نیازمند مشروعیت است که قصد دارد طبق ماده ۵ این پیمان، آن را اجرایی کند. البته درنبرد روسیه و اوکراین، برخی از کشورهای این پیمان به کمک اوکراین آمده اند و توانایی‌ها و قابلیت‌هایی را در اختیار آن قرار داده‌اند، (مانند انگلیس و آمریکا) اما حمله سایبری خطرناک یا مخربی که زیرساخت‌های روسیه را فلج کند، به نظر می‌رسد هنوز مشاهده نشده است. همچنین ناتو برای اعمال قوانین بین‌المللی در حوزه سایبری در سال‌های اخیر به تئوریزه کردن و انتشار کتاب مانند دستورالعمل تالین ۲ پرداخته است تا جنبه‌های حقوقی این موضوع را بررسی کند.

۱ . در سال‌های گذشته، در کنفرانس ورشو ، اعضای ناتو متعهد شدند تا در حوزه دفاع سایبری، مجهز شده، شبکه‌های ملی و زیرساخت‌های خود را تقویت کرده و آماده چالش‌های امروزی شوند. این تعهد، تعهد دفاع سایبری یا (Cyber Defence Pledge) نام دارد.

۲ . بسته اساسی ناتو-گرجستان (SNGP) مجموعه‌ای از اقدامات و ابتکارات با هدف تقویت قابلیت های دفاعی گرجستان و توسعه همکاری های امنیتی نزدیک تر و قابلیت همکاری با اعضای ناتو است.



کمپ منافقین

مغلوب دیپلماسی سایبری موفق دولت سیزدهم ایـــران

حمله به کمپ منافقین پاسخ به حملات سایبری علیه نهاد های دولتی ایران است که در چند ماه گذشته با کمک رژیم صهیونیستی رخ داد.

به گزارش کارگروه بین الملل سایبربان؛ قطعا باید گفت یکی از دستاورد های موفق دولت سیزدهم در تحولات اخیر، سیاست خارجی و دیپلماسی سایبری بود که صورت گرفته است.



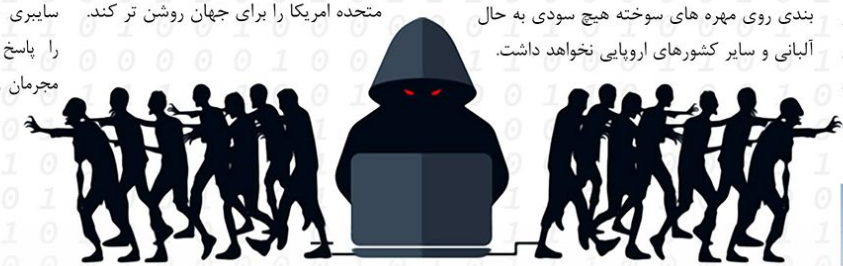
گروهک تروریستی منافقین که از چندی پیش با کمک برخی از دشمنان به ویژه رژیم صهیونیستی و ایالات متحده آمریکا، حملات سایبری به برخی نهاد ها و سازمان های دولتی انجام داده بود حالا در برابر دیپلماسی سایبری جمهوری اسلامی ایران شکست خورده است.

هرچند در این میدان حق پاسخ گویی به حملات صورت گرفته هنوز برای ایران محفوظ مانده است. جمهوری اسلامی ایران که در چندین ماه اخیر درگیر جنگ ترکیبی سنگینی از سوی دشمنان بود، بسیاری از محاسبات را از اساس برهم زد و بار دیگر در مقام دفاع خوش درخشید. در این میان اما گروهک منافقین را باید یکی از مهمترین آلت دست های دشمن و از ارکان اصلی رخداد های اخیر نیز بر شمرد.



حملات سایبری به نهاد ریاست جمهوری ایران، حملات سایبری به وزارت امور خارجه ، حملات سایبری به صدا و سیما و شبکه اینترنتی تلوبیون، آموزش و حمایت از کانون های شورشی، برنامه های ترور، خرابکاری ها و لیدری آشوب ها و اغتشاشات و ... از جمله اقدامات تروریستی این گروهک است که با دیپلماسی موفق ایران، امنیت پوشالی این گروهک از هم گسیخت و موجودیت آنها توسط این حمله بار دیگر زیر سوال رفت و در نهایت تیرانا را مجبور به فهم این نکته کرد، شرط بندی روی مهره های سوخته هیچ سودی به حال آلبانی و سایر کشورهای اروپایی نخواهد داشت.

ایران اگر چه کمی دیر اما با این اقدامات دیپلماسی سایبری و ارسال اسناد و مدارک اقدامات متعدد تروریستی منافقین، فرصتی را برای آلبانی فراهم آورد تا با بررسی این اسناد ، بر علیه این گروهک اقدام کند و به مقر آنها حمله کند. در نتیجه حمله به کمپ اشرف ۳ ، هزاران برگ سند از اقدامات منافقین، کشف و ضبط شد و سیستم های کامپیوتری و ابزار های جاسوسی متعددی جمع آوری شده است که می تواند برهم زننده بسیاری از برنامه های سرویس های سه گانه دشمن شود و در نهایت ماهیت کثیف این فرقه و همکاری آنها با رژیم صهیونیستی و ایالات متحده امریکا را برای جهان روشن تر کند.



باید منتظر بود و دید که پلیس اینترپل بر اساس این جرایم سایبری و اسنادی که از سیستم های منافقین افشا می شود، آنها را تحت تعقیب جهانی قرار خواهد داد یا خیر؟ اقدامات خیلی خوب و بی نظیر دستگاه دیپلماسی سایبری ایران در عملکردی حرفه ای و بی سابقه ، این پیام را به دنیا مخابره کرد که مجرمان سایبری علیه ایران دیر یا زود تحت تعقیب جهانی قرار خواهند گرفت و تاوان سختی در انتظار آنها خواهد بود. درسی که ماجرای کمپ اشرف ۳ برای دشمنان جمهوری اسلامی ایران داشت این نکته است که ایران هیچ تهدید و حمله سایبری به نهادها و زیرساخت هایش را تاب نمی آورد و با دیپلماسی سایبری موفق و پیگیری های حقوقی هر اقدامی را پاسخ گفته و در زمان مناسب مهاجمان و مجرمان را به دادگاه قصاص و محاکمه می کشاند.

آیا کشور های دیگر از این اقدام ایران درس عبرت خواهند گرفت ؟

ایران مهاجمین سایبری را هرگز رها نخواهد کرد.



آیا در تنش سایبری میان آلبانی و ایران که منجر به قطع روابط دیپلماتیک در سال گذشته شد، پای روسیه در میان بوده است؟

ایران وحملات سایبری



تیم واکنش اضطراری رخدادهای کامپیوتری اوکراین (CERT-UA) زیر نظر سرویس ارتباطات ویژه دولتی و حفاظت اطلاعات، به تازگی حملات فیشینگی را که توسط گروه هکری ای.پی.تی ۲۸ (APT۲۸) که با نام های پاون استورم (Pawn Storm)، فنسی بیر (Fancy Bear)، بلودلتا (BlueDelta) انجام‌شده بود، کشف کرد. همچنین این حملات به‌منظور دستیابی به اطلاعات احراز هویت برای ورود به‌حساب کاربری ایمیل، توسط اداره اصلی ستاد کل نیروهای مسلح روسیه انجام‌شده است. طبق این گزارش، هکرها فایل‌های اچ.تی.ام.ال (HTML) را از طریق وب‌سرویس‌های پستی (Ukr.net و Yahoo.com) ارسال کرده و استخراج داده‌های احراز هویت توسط قربانی را با استفاده از درخواست های اچ.تی.تی.پی پست (HTTP POST) اجرا می کردند. همچنین، تیم واکنش اضطراری رخدادهای کامپیوتری اوکراین متوجه شد که یکی از ایمیل هایی که به آن حمله شده متعلق به سفارت ایران در آلبانی، yahoo.com@۱۳۵۷_iri، است.

تیم واکنش اضطراری رخدادهای کامپیوتری اوکراین افزود:

«می‌توان نتیجه گرفت که گروه ای.پی.تی ۲۸، که فعالیت‌های آن توسط اداره اصلی ستاد کل نیروهای مسلح روسیه هدایت می شود، در ماه می ۲۰۲۳، حمله سایبری را علیه نهاد دیپلماتیک خارجی ایران انجام داد».

همچنین در چهارشنبه ۱۶ شهریور ماه سال ۱۴۰۱مصادف با ۷ سپتامبر ۲۰۲۲، دولت آلبانی تصمیم به قطع روابط دیپلماتیک با ایران گرفت و ۲۴ ساعت مهلت داد تا تمامی پرسنل دیپلماتیک و اداری، فنی و امنیتی، کشور را ترک کنند. روز بعد گزارش شد که کارکنان سفارت را ترک کرده و ساختمان توسط بخش خنثی‌سازی پلیس آلبانی تصرف شد.

باید خاطر نشان کرد که «در ۱۵ جولای ۲۰۲۲، آلبانی هدف یک حمله سایبری گسترده با هدف تخریب زیرساخت دیجیتال دولت ، فلج کردن خدمات عمومی و سرقت داده‌ها و اطلاعات تماس الکترونیکی از سیستم‌های دولتی قرار گرفت».

پس از این ادعا کاخ سفید اعلام کرد، آمریکا به این نتیجه رسیده است که ایران مسئول حمله سایبری پانزدهم ژوئیه (۲۴ تیر ۱۴۰۱) و عملیات هک کردن متعاقب آن علیه آلبانی است.

وزارت خارجه ایران هم بلافاصله در بیانیه‌ای اتهامات تیرانا را رد کرد و اعلام کرد: ایران هم به‌عنوان یکی از کشورهای هدف حملات سایبری به زیرساخت های حیاتی خود، هرگونه استفاده از فضای سایبری به‌عنوان ابزاری برای حمله به زیرساخت های حیاتی سایر کشورها را مردود می‌داند و محکوم می‌کند.





حمله هکری به سرورهای بنیاد شهید

حملات سایبری

بنیاد شهید و امور ایثارگران در پی حمله سایبری به سامانه‌های ایثارگران اطلاعیه ای صادر کرد.

در ماه قبل اخباری مبنی بر هک شدن سرورهای بنیاد شهید و امور ایثارگران در فضای مجازی منتشر شد. بر پایه این گزارش، یک گروه هکری به نام **«بختک»** مسئولیت این اقدام را بر عهده گرفت و مدعی شد تمام سیستم‌ها، اطلاعات و پشتیبان‌گیری های ستاد مرکزی را حذف کرده است. بنیاد شهید و امور ایثارگران در پی حمله سایبری به سامانه‌های ایثارگران اطلاعیه ای صادر کرد که متن آن به شرح زیر بوده: همزمان با جا به جایی صورت گرفته در ساختمان ستاد مرکزی بنیاد شهید و امور ایثارگران و تغییرات ایجاد شده در زیرساخت های حوزه فناوری اطلاعات، در ماه گذشته سامانه های اینترنتی این بنیاد با حملات سایبری رو به رو شد که این حملات در همان دقایق اولیه مورد رصد کارشناسان فنی قرار گرفته و کنترل گردید. با توجه به اقدامات صورت گرفته توسط کارشناسان فنی، از خانواده بزرگ ایثارگران تقاضا می شود ضمن صبوری برای راه اندازی مجدد سیستم ها و سامانه ها، اخبار را از رسانه های رسمی پیگیری کرده و همچنین از رسانه ها تقاضا می شود اخبار مربوط به این موضوع را از سوی مبادی رسمی بنیاد شهید و امور ایثارگران مخابره نمایند. سامانه‌های اطلاع‌رسانی و خدماتی پس از بررسی های دقیق و اطمینان از امنیت کامل مجددا در اختیار جامعه ایثارگری قرار خواهند گرفت و روند شفافیت در فعالیت های بنیاد شهید و امور ایثارگران به منوال قبل استمرار خواهد یافت.

توضیحات رئیس بنیاد شهید در مورد هک شدن سامانه های بنیاد شهید امیرحسین قاضی زاده هاشمی گفت:

ما اطلاعات حساس و راهبردی نداشتیم زیرا ما اساسا یک سازمان خدماتی هستیم. از بی سلیقگی هکر ها تعجب کردم. با حمله سایبری که به سامانه های بنیاد شهید شد فرایند های الکترونیکی بنیاد شهید مختل شده و فرایند های کاغذی مجددا برقرار شده است.

انتشار فایلهای شبکه بنیاد شهید توسط گروه هکری بختک

بلا فاصله‌گروه هکری بختک فایل‌های بنیاد شهید را بصورت عمومی منتشر کرد!

از جزئیات بازسازی سرویس بهداشتی و فاکتور تعمیر یخچال گرفته تا توپولوژی دقیق شبکه WAN و صورت جلسات مدیران و مکاتبات محرمانه با سایر ارگانها و کپی شناسنامه و... متاسفانه وقتی یک سازمان هک می شود سایر سازمانها هم متاثر گشته و مکاتبات انجام شده با آنها هم افشا می گردد. اسناد زیادی وجود دارد که اثبات میکند در حال حاضر سازمان‌های زیادی قابل نفوذ هستند و می شود در سطح Admin از راه دور دسترسی ایجاد کرد. این روزها آسیب پذیری های بحرانی زیاده شده است. باید مراقب بود زیرا پس از هک دیگر کاری نمی شود کرد...





استقلال، پرسپولیس و جرایم سایبری

سایبر ورزش

ادبیات فرافکنیِ کانال های هواداری تیم های فوتبال چند وقتی است که فضای مجازی را احاطه کرده است.

ورزش در کشور ما متاسفانه سال هاست درگیر حواشی زیادی است که در سایر نقاط دنیا کم نظیر یا بی نظیر است. مسئله استفاده از رانت و تخلفات از قانون و مافیای فوتبال ، بیش از پیش ورزش کشور را تحت الشعاع قرار داده است. در این بین موضوعاتی که ما را بر آن داشت تا به این خبر بپردازیم، مسئله جرایم سایبری وابسته به دو باشگاه فوتبال استقلال و پرسپولیس است.

بررسی ها نشان می دهد تنها مواردی که از جرایم سایبری فوتبال مهم جلوه کرده موضوع قمار در سایت های شرط بندی بوده است. ضمن اینکه این مسئله دارای اهمیت بسیار بالایی بوده و شکایت ها و پیگیری های هم صورت گرفته است .

مجازات شرط بندی در فضای مجازی

در قانون مدنی مطابق با ماده ۶۵۴ قانون مدنی قمار و گروه‌بندی باطل و دعاوی راجع به آن مسموع نخواهد بود؛ یعنی در جرگه معاملات نامشروع قرار گرفته و طرح دعاوی در رابطه با آن وجاهت قانونی ندارد و قابل پی‌گیری نخواهد بود.

هر فردی که بخواهد در فضای مجازی به امر خلاف مجازات شرط بندی بپردازد بر اساس قانون مجرم است با آن فرد و سایت اینترنتی باید برخورد شود. در نتیجه سایت تعطیل و گردانندگان آن با عنوان مجرمانه قمار محاکمه خواهند شد. کارگروه تعیین مصادیق محتوای مجرمانه در چهل و هشتمین جلسه خود، برخورد با قمارخانه‌های مجازی در اینترنت را به تصویب رساند و آن را به موارد محتوایی که برای ارتکاب جرایم رایانه‌ای به کار می رود (محتوا مرتبط با جرایم رایانه‌ای) اضافه کرد.

اما جرایم سایبری مربوط به فوتبال به همین جا ختم نمی گردد...



بار دیگر این خلا در حاکمیت سایبری کشور حس می شود که این فضا به درستی رصد نشده و قوانین سایبری در این قضایا نقض گشته است. برای مثال کانال های تلگرامی هواداری استقال و پرسپولیس هر دو در مواردی دست به تخلفات واضح و آشکار زده اند که هیچ مرجع قضایی به آن ورود نکرده و هیچ هشداری هم در این موارد صادر نشده است! ممکن است که کانال های فوق تحت نظارت مستقیم از طرف این دو باشگاه نباشد اما وابستگی های آنها به باشگاه های مذکور بدیهی و غیر قابل انکار است.

این کانال ها تبلیغات رسمی قبول کرده و شماره حساب های بانک های داخلی را رد و بدل می کنند پس به احتمال زیاد از داخل کشور مدیریت می شوند. تخلفات این کانال ها در فضای مجازی در درجه اول توهین های مکرر به حاکمیت بوده و در درجات بعد توهین به اشخاص و ترویج و تبلیغ مواردی همچون قمار و فحشا و سایت های شرطبندی و ... بوده است.

توهین به روحانیت، توهین آشکار به حاکمیت و پرسنل باشگاه پرسپولیس با عنوان "طویله آخوندی" ، اهانت های رکیک به سید حجت کریمی سرپرست سابق استقلال، تبلیغ لوازم و لباس های جنسی ، تبلیغ خرید و فروش وی پی ان ها و نقل قول هایی از کسانی که به وطنشان پشت کرده اند از مصادیق بارز جرایم در فضای مجازی است که در این کانال ها منتشر شده است. این فرافکنی ها درعرصه ورزش تبعات سنگینی را به همراه خواهد داشت و موجب ناهنجاری ها و ترویج فرهنگ نادرست در جامعه ما می شود.





شبکه های اجتماعی
حاکمیت سایبری

نظارت پلتفرم های آنلاین چین بر اطلاعات کاربران

اداره فضای سایبری چین (CAC)، به تازگی در دستورالعملی، پلتفرم‌های آنلاین را موظف کرده تا بر صفحات و کاربرانی که اطلاعات نادرست و چالشی منتشر می‌کنند، نظارت کند.
در اطلاعیه اداره فضای سایبری چین آمده است که پلتفرم‌های آنلاین باید بر روی حساب‌های کاربری که اطلاعات اشتباه منتشر می‌کنند یا موضوعات داغ را به شیوه نامناسب و مضر مورد بررسی قرار می‌دهند، نظارت کنند و آنها را به حالت تعلیق در آوردند.
در سیزدهمین دستورالعمل که مربوط به هفته گذشته است جزئیات خاصی در مورد نوع محتوایی که مضر یا غیر قانونی بود ذکر نشده بود اما گفته است که این مسئولیت ارائه دهندگان پلتفرم است تا مدیریت حساب‌ها را بیشتر و تقویت کنند .از جمله الزامات برشمرده شده، تأیید بهتر حساب‌ها و برچسب‌گذاری شایعات یا محتوای بحث‌برانگیز و ساده‌سازی الگوریتم برای ترویج محتوای بیشتر است که شایعات را از بین می‌برد. این سند به اپراتورهای پلتفرم دستور می دهد تا به شدت تولیدکنندگان محتوا را که اطلاعاتی در حوزه‌هایی از جمله امور مالی، آموزش، رسانه و بهداشت عمومی تولید می‌کنند تأیید کنند. این امر بعد از اینکه چین پیش‌نویس دستورالعمل‌هایی که در روز جمعه بر روی تولید کنندگان خدمات آنلاین منتشر کرد صورت گرفت تا محتوای آزار و اذیت سایبری را تحت تهدید جریمه هایی که طبق قوانین موجود برای امنیت آنلاین و حفاظت از داده‌های شخصی می تواند وضع شوند، تحت فشار قرار دهند.

و اما پیام‌رسان «بله»

تأیید رصد اطلاعات کاربران توسط پیام رسان «بله» پس از انتشار تصویر جنجالی!
در فصلی که گذشت تصویری جنجالی در فضای مجازی از یک صفحه کامپیوتر منتشر شده که نشان می داد پیام‌های ارسال‌شده در یک گروه برای کارمندان پیام‌رسان «بله» قابل مشاهده است.
به گزارش کارگروه شبکه های اجتماعی سایبربان به نقل از یک از خبرگزاری‌های داخلی، کاربری اخیراً با انتشار تصویر زیر از یک صفحه نمایشگر کامپیوتر اعلام کرده است کارمندان پیام‌رسان «بله» به پیام‌های کاربران این سکو در گروه‌ها دسترسی دارند. در بیانیه‌ای که مسئولان «بله» در واکنش به این تصویر منتشر کرده، تاکید شده است امنیت و داده‌های شخصی کاربران، جز خطوط قرمز این پیام‌رسان است و «بله» از حریم خصوصی کاربران حفاظت می‌کند و خواهد کرد.



اهمیت نظارت بر پلتفرم های داخلی
به دلیل نقض حقوق کابران در پیام رسان (بله)

تصویر جنجالی از پیام‌رسان «بله»؛ واکنش گردانندگان این پیام‌رسان چه بود؟
این اتفاق در حالی رخ می‌دهد که پیام‌رسان «بله» موفق شد در جشنواره فاوا جایزه بهترین پیام‌رسان داخلی را از آن خود کند. پیام‌رسان «بله» در بیانیه خود عنوان کرده این مواردی که در تصویر منتشر شده پیرامون محتواهای عمومی کانال‌های بیش از هزار کاربر است که محتوای آن‌ها از سوی سایر کاربران به عنوان محتوای نامناسب گزارش شده و از طرف پیام‌رسان مذکور مورد بررسی قرار گرفته است. بخشی از بیانیه پیام‌رسان «بله» در راستای انتشار این تصویر جنجالی بدین‌گونه است:

بله، به عنوان یک پلتفرم، مانند تمام پلتفرم‌های دیگر موظف است تدابیر لازم را برای جلوگیری از کلاهبرداری‌ها و حفظ امنیت، دربارهٔ فعالیت کاربران خود در پلتفرم، اتخاذ کند. از این رو طبق سند قوانین و شرایط استفاده از بله که در قوانین و شرایط استفاده از پیام‌رسان بانکی بله منتشر شده «برای کانال‌ها و بازوهایی که به صورت عمومی در دسترس هستند، بله از الگوریتم‌های خودکار برای آنالیز پیام‌ها برای جلوگیری از انتشار محتوای مجرمانه استفاده می‌کند. همچنین کاربران می توانند در صورت مشاهدهٔ این موارد، گزارش آن را به بازوی پشتیبانی ارسال یا از گزینه «گزارش محتوای نامناسب» استفاده کنند.

بیانیه پیام رسانه بله

به نقل از گردانندگان پیام‌رسان «بله»، گزارش‌های مشکوک مورد بررسی قرار می‌گیرند و در صورت تایید مجرمانه بودن، با آن‌ها برخورد قانونی خواهد شد. گفتنی است با گروه‌هایی که بیش از هزار عضو داشته باشند، در دایره بررسی محتوا، به‌مانند کانال های عمومی رفتار می‌شود. در پایان این بیانیه، مسئولان پیام‌رسان مزبور مجدد تاکید می‌کنند حریم خصوصی کاربران خط قرمز «بله» است و با تمام وجود از آن حفاظت می‌کند. این پیام‌رسان همچنین اذعان کرد که حق قانونیِ پیگیری و برخورد با منتشرکنندگان این تصویر را برای خود محفوظ می‌دارد.



بازی واقعیت مجازی مخاطرات



مصاحبه اختصاصی با کارگردان تور واقعیت مجازی آقای احمدرضا امینی

مصاحبه اختصاصی سایبربان



احمدرضا امینی متولد ۱۳۶۵ در شهر تهران است؛ او که تحصیلاتش را در رشته مخابرات به پایان برده، کارگردان تور مجازی ۳۶۰ درجه بوده و در این زمینه بسیار صاحب سبک و موفق ظاهر شده است. او البته در این مسیر به گفته خودش کارهای مختلفی انجام داده مانند: خبرنگاری، عکاسی خبری، تدوین، امدادگری، راه اندازی کسب و کار در زمینه تعمیر کامپیوترهای مردم از راه دور، خدمت افتخاری و غیر رسمی در حرم رضوی در خصوص بیسیم های حرم بخشی از کارهای او هستند.همچنین به ثبت رساندن ۶ اختراع از جمله فعالیت هایی بوده که در این سال ها انجام داده است. در ادامه مصاحبه سایبربان با وی را بخوانید.

از چه زمانی شروع به فعالیت در زمینه واقعیت مجازی کردید و چه چیزی باعث شد در این زمینه فعالیت کنید؟

از سال ۹۰ به صورت تجاری آغاز به فعالیت کردیم، ابتدا با طراحی سایت برای مشتری ها شروع به کار کردیم اما مشتریان درخواست فراتری نسبت به موارد مشابه داشتند و می خواستند در زمینه رسانه خلاقانه و تاثیرگذار تر باشند که پس از برنامه ریزی و تشکیل یک گروه، اولین بار برای یک برند عینک سازی تور مجازی فروشگاه را آماده کردیم و سپس از لحاظ فنی، کیفیت و ... کار را گسترش دادیم.



شش اختراع به نام شما ثبت شده، این اختراعات چیست و در مورد این اختراعات و کاربرد های آنها توضیح دهید؟

یکی از اختراعات به صورت غیر مستقیم مربوط می شد به سازمان آتش نشانی تهران در بافت های سنتی مثل بازار تهران که در مسیریابی دچار مشکل هستیم. به همین دلیل تحقیقاتی در زمینه واقعیت مجازی صورت گرفت و تصویربرداری از بازار تهران به کمک سازمان آتش نشانی انجام شد و این بررسی ها و تحقیقات منجر به ثبت اختراعی به نام "مسیریابی در بافت های تاریخی شهری به لحاظ امدادی" شد و در جلساتی هم برای مدیران سازمان آتش نشانی این اختراع ارائه شد. اما به طور کلی مورد حمایت قرار نگرفت و در مجموعه های اداری ما متاسفانه معاونت ها به یکدیگر کمک نمی کنند تا یک کارگروهی قوی به سرانجام برسد و این موضوع مانع رشد و خلاقیت میگردد؛ دلیل آن هم بخاطر ضعف در آموزش است اما همچنان امیدواریم با اصلاح نظام آموزشی این موانع برطرف شود.

اختراعات دیگر در زمینه مخابرات الکترونیک، حوزه امنیت و توانبخشی بود که برای مثال: دستگاه پول شمار هوشمند نوری برای نابینایان که توانایی شمارش اسناد، پول و موارد مشابه دیگر را در زمانی خیلی کوتاه انجام می داد. نمونه دیگر، کیف حمل اسناد محرمانه بود که برای حامل آن در صورت احساس خطر، توانایی از بین بردن اسناد، مدارک و ... را ایجاد می کرد. کیت مخبر (کد کننده بیسیم های مرزبانی) ، لباس هوشمند برای تنظیم دمای بدن نابینایان و ششمی هم یک نوع لباس هوشمند برای مرزبانی بود که قابلیت شبکه شدن و انتقال حرارت را داشت.

شما اولین گروهی هستید که در این زمینه شروع به فعالیت کردید، ایده اولیه این کار از کجا ایجاد شد؟

در حوزه استفاده متفاوت از هدست های واقعیت مجازی پیشرفته، بیشتر در زمینه سرگرمی، آموزش و ابزار های رایج در متاورس و به این شکل کاربرد دارد. این که برای نجات جان افراد اقدامی صورت گیرد آن هم با استفاده از این هدست ها، اولین بار بود؛ این کار بسیار مورد استقبال فدراسیون های صلیب سرخ جهانی و کشور های همسایه قرار گرفت؛ به طوری که در اولین جلسه ارائه به نمایندگان صلیب سرخ ، آنها از این طرح شگفت زده شدند و در توییتر پیامی با موضوع استفاده از این بازی به همراه تگ کردن نمایندگان صلیب سرخ کشور های دیگر منتشر کردند. ما با تور مجازی ساده شروع به کار کردیم؛ بعدها به تور مجازی حرفه ای "تور مجازی زیر آب و تور مجازی هوایی" ارتقا پیدا کردیم و سازگاری با هدست های متا را در دستور کار قرار دادیم. تولید فیلم ۳۶۰ درجه، انجام جلوه های ویژه روی فیلم ۳۶۰ درجه از دیگر کارهای ما می باشد. اما آنچه که در چند سال اخیر بنده مشاهده کردم، گروه هایی بودند که قبل از ما شروع به فعالیت کردند اما از فعالیت در این زمینه کنار کشیدند. چرا که نگاه دیجیتال محوری از سمت حاکمیت اعمال نشده یا حمایت کافی صورت نگرفته است.

اغلب مدیران شرایطی را قرار می دهند که این شرایط استارتاپ محور نبوده و دولتی محور است و نیاز به مدارکی دارند که موجب محدودیت های بیشتر می شود. در بحث های فنی طراحی بازی های ساخته شده در زمینه طراحی بافت مثل سنگ، چوب و دیوار یک مقدار فضا به صورت کارتونی بوده چون سفارش دهنده، حمایت کننده کار نبوده و هزینه های بالایی برای انجام این طراحی ها نیازهست. اما در کل تا به حال چندین جا این بازی را ما به مسئولین ارائه کرده ایم و آنها گفتند که از کیفیت بالایی برخوردار بوده است.



اقدام به تولید واقعیت مجازی حرم امام رضا (ع) چگونه آغاز شد و تا به حال در چه مکان های مقدسی این فعالیت صورت گرفته است؟

در مجموعه حرم امام رضا(ع) مراسم های خاصی برگزار می شد که مردم استقبال می کردند، همانطور که در قبل عرض کردم ما فعالیت خود را به واقعیت مجازی پیشرفته گسترش داده بودیم و در عین حال خلاء زیارت مجازی موجود بود، بنده علاقه مند بودم که در این زمینه فعالیت شود. مدیریت وقت آستان قدس این کار را سفارش دادند و توانستیم با اضافه کردن تصاویر هوایی سه بعدی حرم و ارتباط با سامانه های مختلف آستان قدس، زمانی که در های حرم بسته شد این کار را انجام دهیم. رونمایی این کار در زمان کرونا صورت گرفت و ضبط تصاویر بیش از دوسال به طول انجامید و موازی با این فرایند پردازش ها هم صورت گرفت که به دلیل عدم همکاری مسئولین مالی و نگاه سنتی، با وجود تهیه سرور ها، ترافیک های ۱۰ ترابیتی در ماه و هزینه های شخصی توسط گروه ما، متاسفانه هزینه و دستمزدی به گروه ما پرداخت نشد! در حال حاضر هم تمامی حرم ها به جز سوریه زیارت مجازی دارند که با جستجوی واژه "زیارت مجازی" در موتورهای جستجو می توانید کارهای گروه ما را مشاهده کنید.



واقعیت مجازی و ارتباط آن با بلایای طبیعی که ساخت بازی مخاطرات را رقم زد، ایده چه کسی بود ؟ مشکلات و فرایند پردازش آن را توضیح دهید.

بعد از زلزله بم ، بنده خیلی تحت تاثیر این حادثه قرار گرفتم، عضو جمعیت هلال احمر شدم و ماموریت هایی را تجربه کردم، تا این که بعد از فروریختن ساختمان پلاسکو با انجام هماهنگی ها با سازمان های مربوطه، فیلم برداری سه بعدی صورت گرفت که موجب کمک زیادی به مجموعه های امدادی، جلوگیری از تکرار اشتباهات و پیشگیری های لازم در موارد بعدی شد. این فرایند به صورت تصاویر ۳۶۰ درجه و تورمجازی صورت گرفت که تصاویر ۳۶۰ درجه در گوگل بارگذاری شد و در بازخورد ها حتی آتش نشان هایی از کشور انگلیس و برخی کشور های دیگر از این تور بازدید کردند و در بازه سه روز، شصت هزار بازدید از این تصاویر ثبت شد. معاونت آموزش و پژوهش هلال احمر عنوان کرد که فدراسیون صلیب سرخ جهانی حمایت هایی را برای طرح های برتر که می تواند به رشد نوع آموزش و اثرگذاری مطلوب در این حوزه کمک کند، در نظر خواهد گرفت و ما توانستیم با همکاری هلال احمر این طرح را آماده کنیم. اما پس از ارسال طرح تا الان هنوز هیچ بودجه ای در اختیار ما قرار نگرفته است، البته پس از تحویل بازی مخاطرات باز هم در مسائل اداری دچار مشکلاتی بودیم و هستیم.

با چه ارگان هایی تعامل داشته اید؟ حمایت ها از شما چه گونه بود ؟

تیم ما در حال حاضر حمایت خاصی از سازمان یا ارگانی نشده اما آمادگی این را داریم با توجه به نیاز ها، محتوا و سناریو آماده کنیم. برای مثال یکی از شرکت های زیر مجموعه ایران خودرو از ما خواست که یک کار با کیفیت دو زبانه انگلیسی- فارسی آماده شود که قابلیت جذب شرکای خارجی، فروش ارزی، و موارد دیگر را به همراه داشته باشد.



چه ایده ای در زمینه مخابرات و جنگ الکترونیک در حال حاضر دارید؟

به نظر بنده در گذشته اکثر توان جنگال روی این موضوع بود که تجهیزات جنگنده دشمن را مختل کنند یا پهپاد ها را رهگیری کنند و کارهایی از این قبیل اما هدف از این کارها چه بوده؟ این که در جنگ، نیروهای نظامی دشمن درگیر شده و شکست بخورند. اما درحال حاضر موضوع متفاوت شده و تئوری ها تغییر کرده است و نظریه جدید در جنگ ها می گویند هیچ نیاز آنچنانی به لشکرکشی و استفاده از سلاح های گوناگون نیست بلکه اگر شما یک مساحت دو و نیم اینچی به اسم مغز ساکنین کشور دشمن را تحت تاثیر قرار بدهید یا تصرف کنید، شما برنده جنگ خواهید بود. به نظر شخصی بنده پلتفرم متاورس ملی می تواند سر منشأ اثر در این حوزه باشد، چون استاندارد های موجود در متاورس بین الملل برخی مواردش در کشور ما قابل پیاده سازی نیست و ممکن است حاکمیت داده را به خطر بیاندازد؛ ولی ظرفیت های بالایی وجود دارد که با یک زیرساخت امن و بومی در این عرصه از نظر تولید محتوا،آگاهی در زمینه سایبری و بروزرسانی در رسانه و رسانه های نوین بتوانیم این فناوری را بومی کنیم. با متاورس ملی می شود در بسیاری از هزینه های جنگی صرفه جویی شود البته به شرط سپردن کار به متخصصین نه به مافیاها و کاسب ها !

کدام دوره را در وزارت ارتباطات و فناوری اطلاعات مفید تر ارزیابی میکنید؟

با این که بنده اصلا طرفدار ایشان نیستم، به نظرم دوره آقای آذری جهرمی فعالیت رسانه ای پر هیاهو تر ظاهر شد، در حال حاضر با توسعه فیبر نوری و موارد دیگر، اقدامات خاصی در رسانه صورت نگرفته و با توجه به شرایط فعلی که پلتفرم های خارجی در کشور محدود شده است خیلی اثرگذاری خاصی را شاهد نبوده ایم.



کدام نهاد ها و ارگان ها را کم کارتر و مانع پیشرفت در این حوزه می دانید؟

بنده دسترسی به داده های دستگاه ندارم اما اگر بخواهم از دانشگاه ها شروع کنم، نگاه استارتاپ محور و ارتباط با صنعت بسیار کم وجود دارد، اگر این روند ها اصلاح شود و با وجود هوش مصنوعی و راه های ارتباطی پیشرفته ، دانشگاه ها می توانند بسیار سر منشأ اثر باشند. ما مدتی است که با وزارت نیرو در بخش تولید برق حرارتی وارد مذاکره شده ایم، خیلی از افراد که در این حوزه فعالیت می کنند ممکن است به این فرایند و سختی های زیادی که در تولید و انتقال برق وجود دارد آگاه نباشند، حدود ۸۰ درصد از برق کشور با این روش تولید می شود که موجب صرفه جویی های ارزی شده و چقدر این امکان وجود دارد که گروه هایی برای آموزش در این مکان ها حضور داشته باشند؛ اما با استفاده از واقعیت مجازی می توان در بحث های آموزشی و فرهنگ سازی و ... فعالیت هایی را به اجرا گذاشت که بسیار موثرتر باشد.





مصاحبه اختصاصی سایبربان با مهدی بکایی پیرامون بازار محصولات اپل در ایران و ماجراهای پشت پرده رجیستری آیفون ۱۴

مصاحبه اختصاصی سایبربان

مهدی بکایی متولد سال ۱۳۵۷ در شهر مقدس قم، یکی از اولین افرادی است که نشانگان تجاری اپل را به بازار ایران معرفی کرد، او پس از سال‌ها فعالیت در این حوزه، نظرات قابل تأملی پیرامون فعالیت‌های اپل در ایران دارد. در ادامه مصاحبه سایبربان با وی را بخوانید.



لطفاً درباره سابقه حضور اپل در ایران توضیحاتی را برای مخاطبان سایت ارائه دهید

من در سال ۱۳۷۸ واردعرصه بازار اپل شدم و در ابتدا با محصولات صوتی مانند آیپاد که دارای طراحی خاص و کیفیت صدای بی نظیری بود، شروع به فعالیت کردم. محصولات اپل در ایران هنوز جا نیفتاده بود و فقط افراد حرفه ای در بخش صدا و تصویر از این محصولات استفاده می کردند. همانطور که می دانید اپل تنها شرکت در دنیا است که محصولات نرم افزاری و سخت افزاری را خودش طراحی می کند و این نکته بسیار حائز اهمیت است. یکی از دلایلی که مرا به سمت بازار محصولات اپل برد همین موضوع بود، چون برای بخش حرفه ای جامعه بسیار مفید بود و به صورت یک محصول عمومی شهرت نداشت.اپل سال ها فعالیت داشت تا زمانی که آیفون معرفی شد و این همه گیری به ویژه در ایران، اتفاق افتاد.

چون محصولات اپل از جمله نوت بوک و آی مک، سی پی یو مخصوص خود را داشت به همین دلیل یک دو قطبی جذاب در بازار ایجاد کرده بود و محصولات ویندوز و اپل را کاملا از هم متمایز کرده بود. با گذشت زمان اپل در سال ۱۳۸۲ سی پی یو اینتل را ایجاد کرد که هم زمان دو سیستم عامل را در بر می گرفت و همین موضوع باعث شد تا از نظر"نرم افزاری" نگرانی های موجود برطرف شود. واردات محصولات اپل در ابتدا به صورت مسافرتی و بدون جعبه با قیمت های بسیار گزاف توسط یک یا دو شرکت که نام نمی برم، صورت می‌گرفت و به صورت رسمی در جریان نبود.

بعدها در شروع فعالیت تجاری ام، برخی افراد با ما تماس گرفته و مدام شکایت می کردند که چرا محصولات در بازار با این قیمت ها عرضه می شود در اولین اقدام قیمت ها را کاهش دادیم و با یک سود معقول و مناسب، فعالیتمان را شروع کردیم، در این زمینه تا به امروز مشغول هستم اما در سال ۱۳۹۵ تقریباً شبه بازنشسته شدم، چرا که یک سیستمی بر مبنای قدرت و ثروت ایجاد شد و مقابله با این سیستم دیگر ممکن نبود، تنها به چند شرکت مجوزهای فروش را دادند که این موضوع از آیفون ۷ به بعد همراه با آغاز رجیستری شروع شد.

اولین شرکتی که در نمایشگاه الکامپ با محصولات اپل حضور داشت ما بودیم که مورد استقبال مردم قرار گرفت. اما هدف اصلی ما از ورود به بازار اپل، کیفیت بالا، سیستم نرم افزاری فوق العاده قوی، حرفه ای و کاربردی و عمر طولانی مدت و بدون دردسر آن بود. مثلا یک محصول اپل را حدود ۱۰ سال می توان استفاده کرد.

به نظر شما چند درصد از مردم ایران به دلیل مد بودن از محصولات اپل استفاده می کنند؟

بخش اعظم اپل مد بودن آن است، و حداقل ۵۰ درصد افراد به همین دلیل این برند را انتخاب می کنند، زیرا همان نشان سیب اپل بیانگر یک سطح بالا در جامعه است و برخی افراد حتی پول قرض می گیرند تا این محصول را تهیه کنند. این اتفاق نه تنها در ایران بلکه در همه جا هست اما در کشور های جهان سوم بیشتر مشهود است. اپل در حال حاضر چند درصد از بازار ایران را در اختیار دارد؟ آیا هر آن چه در سبد محصولات اپل وجود دارد در ایران موجود می باشد؟

همه محصولات اپل در بازار ایران موجود است. تفکیک محصولات اپل در ایران به دو بخش گوشی و محصولات آی تی مربوط می شود، اما به صورت تخمینی حدود ۳۰ تا ۳۵ درصد از بازار این عرصه در ایران به اپل اختصاص دارد.

آخرین وضعیت رجیستری آیفون ۱۴ در ایران به چه شکلی است؟

یک طرح و یک اتفاق ویژه در کشور ما رخ داد بنام رجیستری تلفن همراه، یکی از بهترین طرح های کنترلی ممکن بود، دولت هم کمک بزرگی به مردم کرد، آن هم این بود که اپل ۱۲ ماه محصول را گارانتی میکرد ولی در کشور ما ۱۸ ماه گارانتی می شد. متاسفانه ما داریم بعضی از خطاها را تکرار می کنیم، به برخی از شرکت ها با در نظرگرفتن المان های مخصوص مجوز داده شده است. هر گوشی پس از روشن شدن یک IMEI دارد و با این طرح رجیستری تکلیف مصرف کننده روشن بود. این طرح به صورت آزمایشی از آیفون ۷ شروع شد و تا آیفون ۱۳ به صورت رسمی به درستی انجام شد

به نظر شما اپل چگونه در برندسازی تا این حد موفق شد؟

بخش اعظم این ماجرا به استثمارگری آمریکا مربوط می شود، نکته بعد اینکه آن ها همیشه در صنعت آی تی در صدر بوده اند البته کره ای ها هم برای مدتی وارد شدند اما باز هم دو شرکت مایکروسافت و اپل بودند که در ظاهر رقابت داشتند و اکثر درآمدها به حساب این دو رفت. برند سازی هدفمند است، چیزی که در کشور ما گم شده و به آن توجهی نمی شود با این که دم از تولید داخلی می زنیم اما حمایتی از دولت ها نمی بینیم. شما فیلمی در هالیوود نمی بینید که از محصولات اپل در آن استفاده نشود. اپل صرفا یک گوشی موبایل نیست، بلکه یک هنر و علم است، یک تخصص برای رسیدن به ثروت وجامعه به جایی می رسد که سرمایه و نقدینگی شرکت اپل از دولت آمریکا بیشتر می شود. در آمریکا هم آزمون و خطا صورت گرفته اما با مدیریت بهتر، اپل سال ها فعالیت داشت مثل هزاران محصولی که در کشور ما خرید و فروش میشد و متاسفانه من تحلیلی در مورد اپل از اقتصاددانان نشنیده ام که چرا اپل اینگونه برند برتر شده است. فروش فقط دلیل اصلی نیست، باید مسئولین ما کنار شعارها در عمل هم حرفی برای گفتن داشته باشند.

.محصولات اپل توسط چه شرکت هایی وارد کشور می شوند؟

در حال حاضر روی محصولات غیر از گوشی هیچ نظارت و کنترلی نیست! اما برای گوشی های تلفن همراه هوشمند، حدود ۷۰ شرکت هستند که زیر نظر وزارت صمت فعالیت می کنند.

اما چه اتفاقی باعث شد آیفون ۱۴ رجیستر نشود؟

در مورد اول گفتند؛ بخاطر دسترسی به اینترنت ماهواره ای است اما این قابلیت در کشور ما وجود ندارد!

در مورد دوم اعلام کردند که گوشی بالای ۶۰۰ دلار اجازه واردات ندارد، اما چگونه تلفن همراه سامسونگ با قیمت ۱۲۰۰ دلار سه روز بعد از معرفی با گارانتی در بازار ایران عرضه شد ! نکته بعد اینکه مگر اپل یک برند آمریکایی نبود، پس چگونه آیفون ۱۳ پرومکس در بازار به مراتب موجود شد، در صورتی که خود اپل این محصول را نداشت اما در کشور ما به وفور در دسترس بود. با این ممنوعیت آماده سازی بستر قاچاق فراهم شد، در صورتی که مسیر ایجاد شده بود و داشتیم درست حرکت می کردیم، اما دوباره به تکرار خطا بازگشتیم. با این کار گارانتی هم از بین رفت، ما چه زمانی از محدود کردن ها و امر و نهی های نادرست به نتیجه رسیدیم؟ الان کسی که آیفون ۱۴ را خریداری کرده می خواهد از تکنولوژی روز دنیا استفاده کند، ما که نمی توانیم جلوی تکنولوژی بایستیم. مورد بعدی این که برخی افراد از فروش آیفون ۱۳ بهره زیادی بردند، چرا باید یک تلفن همراه هوشمند سامسونگ که از نظر قیمت "دلاری" با آیفون برابر هستند، در بازار ایران ۵۲ میلیون تومان فروخته شود اما آیفون حدود ۱۰۰ میلیون تومان باشد! تلفن همراهی که گارانتی دارد پس قاچاق نیست و دولتی وارد شده و قانون را رعایت کرده، پس این تفاوت قیمت محصولات از کجا آمده؟ هیچ شخصی هم پاسخگو نیست، آیفون ۱۵ به زودی عرضه خواهد شد در صورتی که تکلیف آیفون ۱۴ هنوز در کشور ما مشخص نیست. چرا مردم باید تاوان تصمیمات غلط و اشتباه مسئولین را بدهند، مسئولینی که حتی پاسخگوی درست هم نیستند. وزیر ما اسم این برند را به کارنمی برند در صورتی که ۴۰۰ هزار گوشی از این برند وارد کشور شده است.

آخرین وضعیت رجیستری آیفون ۱۴ در ایران به چه شکلی است؟

یک طرح و یک اتفاق ویژه در کشور ما رخ داد بنام رجیستری تلفن همراه، یکی از بهترین طرح های کنترلی ممکن بود، دولت هم کمک بزرگی به مردم کرد، آن هم این بود که اپل ۱۲ ماه محصول را گارانتی میکرد ولی در کشور ما ۱۸ ماه گارانتی می شد. متاسفانه ما داریم بعضی از خطاها را تکرار می کنیم، به برخی از شرکت ها با نظرگرفتن المان های مخصوص مجوز داده شده است. هر گوشی پس از روشن شدن یک IMEI دارد و با این طرح رجیستری تکلیف مصرف کننده روشن بود. این طرح به صورت آزمایشی از آیفون ۷ شروع شد و تا آیفون ۱۳ به صورت رسمی به درستی انجام شد.

داریا همراه و صنعت تولید داخلی تلفن همراه هوشمند

در حال حاضر می گویند تلفن همراه هوشمند ایرانی تولید شده، خب یک سوال؟! یک نماینده از این شرکت بیاید و بگوید کدام قطعه این تلفن همراه هوشمند، ایرانی می باشد؟

ما صنعت خودرو را گذراندیم و مردم دیگر توان تفکر و تحمل این را ندارند که یک اتفاق جدید با این رویه بیفتد، چرا مدام آزمون و خطا می کنیم، آیا ما سی پی یو تولید کرده ایم؟ الان مثل گذشته نیست و مردم با یک سرچ ساده می فهمند، این کارها عواقب دارد و باعث سرخوردگی همه ما می شود .اگر داریا بخواهد با این سیاست که سایربرند ها را با محدودیت مواجه کند خود را مطرح کند، به نظر من قطعاً شکست خواهد خورد.



اما اگر ما سی پی یو تولید کردیم وحتی اگرعالی هم نبود باید تحت حمایت واقع شود. در این دوره چنین اتفاقاتی به خوبی رقم نمی خورد شاید این محصول را در اختیار برخی ارگان ها قرار دهند و فروش هم برود اما این شرایط فروش برابر نیست، بلکه باعث ترویج اقتصاد رانتی شده و شکست خواهد خورد. شرکت ایران خودرو یکی از بدهکار ترین شرکت هاست در صورتی که از آن حمایت های زیادی صورت گرفت. چرا به این حال و روز افتاده؟ همه می دانیم اما درس نمیگیریم، این حرکت در حوزه تلفن همراه هوشمند هم به همین شکل خواهد شد، چون خود این شرکت ها باید در بازار رشد کند نه این که به زور بخواهند آن ها را نگه دارند. در صنعت آی تی هر گونه مقابله ای محکوم به فناست، ما توانستیم جلوی اینستاگرام را بگیریم؟ نه و حتی باعث ایجاد فروش فیلتر شکن هم شدیم، پس صنعت آی تی متفاوت است و دسترسی به آن آسان می باشد. در صورتی که دیدیم کشورهایی که به ظاهر دم از حمایت مردم ایران در ماجراهای سال گذشته می زدند هم در زمینه اینترنت ماهواره ای و اینترنت رایگان و... هیچ کار خاصی نتوانستند انجام دهند.

تاثیرات عدم واردات آیفون ۱۴ بر بازار موبایل چقدر بوده است؟

عدم ارائه گارانتی باعث آسیب دیدن مردم و ورود غیرقانونی ۴۰۰ هزار تلفن همراه آیفون ۱۴ به کشور شد و همچنین ده هزار میلیارد تومان برای دولت خسارت به بار آورد. عجیب تر اینکه پول رجیستری پرداخت می شد، نظارت هم بود، اما این اشتباه صورت گرفت و این اقدام باعث ایجاد شرایط قاچاق شد و طبیعتا به شرکت های دارای مجوز آسیب های بسیاری خواهد رسید.

به نظر شما آیفون ۱۵ این مشکلات را خواهد شد؟

فکر میکنم باید یک کارگروهی تشکیل شود و تکلیف آن دسته از افرادی را که ۴۰۰ هزار گوشی آیفون ۱۴ خریداری کردند، مشخص شود. باید زودتر برنامه ای مشخص شود و اعلام کنند که آیفون ۱۵ رجیستری می شود یا نه و اگر نمی شود چرا به آن در سامانه آنتن داده خواهد شد!

سامانه هوشمند
hamta.ntsw.ir
سامانه هوشمند مدیریت تجهیزات ارتباطی





سایبر اینفوگرافی

ذخیره داده ها بر DNA

سیستم های مغناطیسی یا نوری ذخیرهٔ اطلاعات که در حال حاضر این حجم از اطلاعات صفر و یک را نگهداری میکنند، معمولا بیش از یک قرن دوام ندارند. علاوه بر این، عملیات اجرایی مرکز داده ها انرژی بسیار زیادی مصرف میکند. به طور خلاصه میتوان گفت ما در آستانه یک مشکل جدی ذخیره اطلاعات قرار داریم که با گذشت زمان بدتر می شود.با این حال، پژوهشگران روش دیگری برای ذخیره سازی اطلاعات توسعه می دهند که ذخیره سازی بر پایهٔ DNA است؛داده ها می توانند در توالی این حروف ذخیره شوند و DNA را به شکل جدیدی از فناوری اطلاعات تبدیل کنند.

فعالیت در شبکه های اجتماعی در هر دقیقه

۸۸.۳ میلیون	۳۳.۴ میلیون	۱۵۹.۳ میلیون	۴۹.۷ هزار	۴۷۳ هزار

ایده ی ذخیره سازی اطلاعات روی DNA

دانشگاه هاروارد

در سال ۲۰۱۷، گروه چارچ در دانشگاه هاروارد از فناوری ویرایش DNA کریسپر برای ثبت تصاویر دست یک انسان درون ژنوم- Escherichia coli اشرشیاکلی استفاده شد که با دقتی بیش از 90 درصد خوانده شد.

دانشگاه واشنگتن

پژوهشگران دانشگاه واشنگتن و مؤسسه ی پژوهشی مایکروسافت نیز یک سیستم کاملا خودکار برای نوشتن، ذخیره کردن و خواندن داده های کدگذاری شده در DNA توسعه دادهاند

مایکروسافت

پیشرفت های اخیر در زمینه ی تکنیک های نسل جدید تعیین توالی خواندن آسان و همزمان میلیاردها توالی DNA را امکان پذیر می کند و برای پیگیری نتایج تجربی، از روش بارکدگذاری استفاده می کنند.

توئیست بیوسایِنس

از چالش های رواج ذخیرهسازی اطلاعات در DNA، بحث هزینه ها و سرعت خواندن و نوشتن DNA مطرح می شود که اگر قرار است این روش با ذخیره سازی الکترونیک رقابت کند، باید کاهش بیشتری پیدا کند.

دلایل عدم توانایی در به کارگیری DNA

هزینه ی بسیار زیاد

رمزگذاری یک گیگابایت اطلاعات روی DNA چندین میلیون دلار هزینه دارد. شرکت کاتالوگ امیدوار است که این هزینه را تا ۱۰ دلار کاهش دهد.

جزئیات و صفر و یک داده ها

مشکل اصلی در طراحی سیستم های ذخیره سازی بر اساس DNA مشاهده جزئیات و صفر و یک های داده های باینری و جفت بازهای شیمیایی (AT و CG) است.

مزیت های روش شرکت کاتولوگ

این شرکت بر پایه ی ۱۰۰ مولکول DNA بر اساس جفتهای ده تایی است. این شکل چینش مولکولها به طور مستقیم اطلاعات باینری را رمزگذاری نمی کند و به جای آن چند مولکول کوچکتر DNA را به یک مولکول بزرگتر تبدیل می کند.

هارد درایوهای کنونی به نسبت DNA فضای بیشتری اشغال میکنند. نسبت ذخیره سازی ها در درایو ، حدود ۳۰ میلیون گیگابایت در هر متر مکعب است؛ امّا با روش شرکت کاتالوگ میتوان ۶۰۰ میلیارد گیگابایت را در همان فضا ذخیره کند.

ذخیره سازی اطلاعات با استفاده DNA

ماندگاری بالای اطلاعات

DNA پس از هزاران سال همچنان قابل خواندن است و فضای فوق العاده کمی را نیز اشغال می کند.

ذخیره سازی در فضای کم

تمام اطلاعات دیجیتالی که امروزه در جهان وجود دارد را میتوان در کمتر از ۲۰ گرم DNA ذخیره کرد.

ذخیره اطلاعات باورنکردنی

ذخیره ی اطلاعات به جای صفر و یک از ٤ نوکلئوتید با نامهای A، C، G و T می شوند.

پروژه ای با 3 میلیارد نوکلئوتید

امروزه میتوان DNA هایی شبیه به ژنوم انسان را با حدود 1000 دلار خواند و دستورات ژنتیکی را با استفاده از ابزارهای مصنوعی بیولوژیک نوشت.



تشخیص چهره به کمک DNA

ساخت پایگاه های اطلاعاتی از اسکن ۳ بعدی از چهره افراد

استفاده از روشهای آماری به نژاد ، جنسیت فرد و یافتن ژن های مسئول

دسته بندی شکل چهره، طول و ابعاد با استفاده از مدل رایانشی

تعیین چهره ی آینده ی نسل بشر یا گذشتگان، با استفاده از دی ان ای چهره

مرز بعدی ذخیره سازی داده ها

فناوری ذخیره داده ها

بشریت در حال تولید داده ها با سرعت غیرقابل تصوری است، تا جایی که فناوری های ذخیره سازی نمیتوانند آن را ادامه دهند و در هر پنج سال، مقدار دادههایی که ما تولید می کنیم ۱۰ برابر افزایش می یابد.

تکامل ذخیره اطلاعات

طبیعت یک رسانه ذخیره اطلاعات باورنکردنی - DNA - را تکامل داده است. طرح های اولیه برای ساخت پروتئین های تکامل یافته است، اما DNA میتواند برای اهداف بسیار بیشتری از آن استفاده شود.

فضای کم - عمر طولانی

داده های موجود در صدها هزار دیویدی میتواند در یک بسته DNA به اندازه جعبه کبریت قرار بگیرد. از هارد دیسک های امروزی که ممکن است سال ها یا دهه ها عمر کنند امّا DNA هرگز منسوخ نمیشود.

ذخیره سازی دیجیتال

ایده ذخیره سازی داده های دیجیتال در DNA چندین دهه قدمت دارد، امّا کار اخیر هاروارد و موسسه بیوانفورماتیک اروپا نشان داد که پیشرفت در روش های مدرن دستکاری DNA می تواند رکورد جهانی برای مقدار داده های با موفقیت ذخیره شده در DNA را به ۲۰۰ مگابایت برساند.

ذخیره سازی داده ها

توالی های DNA

واکنش های شیمیایی ساخته شده و هدایت می شوند.آنها را با سایر مواد شیمیایی مخلوط می کنند تا واکنش ترتیب رشته های DNA را، کنترل کنند.

نسخه های پشتیبان

به جای ساختن یک رشته ، واکنش های شیمیایی بسیاری از رشته های یکسان قبل از این که کپی هایی از رشته بعدی در مجموعه بسازند؛ ایجاد می کنند.

خواندن مجدد داده ها

برای بازخوانی داده ها از فضای ذخیره سازی از یک ماشین توالی یابی استفاده می کنیم که برای تجزیه و تحلیل DNA ژنومی در سلول ها استفاده می شود و در صورت حذف داده ها و ایجاد خطا، نسخه های پشتیبان وارد عمل می شوند.

در حال حاضر، اکثر سیستم های بازیابی DNA نیاز به خواندن تمام اطلاعات ذخیره شده در یک ظرف خاص دارند، حتی اگر فقط مقدار کمی از آن را بخواهیم. روش های بیوشیمی امکان دسترسی به اطلاعات خاص را آسان می کند.

مجری طرح: موسسهٔ اطلاع رسانی سایبریان



نمایشگاه هوایی پاریس در سال ۲۰۲۳

Paris Air Show 2023

نمایشگاه هوایی پاریس در سال ۲۰۲۳ (Paris Air Show)، که در ابتدا «نمایشگاه هوایی حرکت هوایی پاریس» نام داشت، پس از ۴ سال وقفه ناشی از بیماری همه‌گیر کرونا، در کاخ بزرگ پاریس از ۱۹ تا ۲۵ ژوئن سال جاری برگزار شد. در نمایشگاه هوایی پاریس ۲۰۲۳ بیش از ۳۰،۴۶۰ شرکت کننده حضور داشتند که شامل ۲۵۰۰ شرکت نمایشگاهی از ۴۶ کشور بود. تقریباً ۵۵ درصد از گروه شرکت کننده از خارج آمده بودند. این رویداد به‌وسیله «SIAE»، یکی از شرکت های تابعه «GIFAS»، انجمن صنایع هوافضای فرانسه سازماندهی شد. با توجه به بهبود شدید سفرهای هوایی تجاری و بازگشت رشد به سطح قبل از کووید در پایان سال جاری، توجه سازندگان هواپیما به افزایش تولید، یافتن کارگران ماهر و پاسخگویی به تقاضای سیری ناپذیر خطوط هوایی معطوف شده که تعدادی از آنها اکنون به حالت خرید بازگشته‌اند.

اگرچه ممکن است معاملات کلان سال گذشته وجود نداشته باشد، اما شایعاتی مبنی بر سفارش احتمالی قریب‌الوقوع ترکیش ایرلاینز در اواخر امسال و همچنین معامله‌ای با شرکت این دی گو «IndiGo» هند، به عنوان بزرگ‌ترین قرارداد خرید واحد در تاریخ حمل و نقل تجاری، وجود داشت. شرکت‌های امیدوار به اعلام محصولات جدید از سوی ایرباس یا بوئینگ، به شکل یک هواپیمای مسافربری جدید از بوئینگ یا یک هواپیمای A۲۲۰ از ایرباس، احتمالاً با تمرکز بر رساندن محصولات موجود به دست مشتریان در این نمایشگاه ناامید شدند. اختلالات مداوم در زنجیره‌های تأمین هوافضای جهانی و کمبود قطعات یدکی بر برنامه خطوط هوایی تأثیر می‌گذارد. تونی داگلاس (Tony Douglas)، مدیرعامل شرکت هواپیمایی جدید عربستان سعودی، ریاض ایر، گفت که از فرصت‌ها و پتانسیل این شرکت هواپیمایی با خدمات کامل، اولین راه‌اندازی در ۲۰ تا ۳۰ سال گذشته، استقبال کرده است.

اگرچه این خط هوایی جدید هنوز ۲ سال با شروع فعالیت فاصله دارد، اما در حال حاضر با سفارش‌های عظیم، جاه‌طلبی‌های بزرگ برای تغییر شکل هوانوردی عربستان سعودی و خاورمیانه و یک بوئینگ ۷۸۷ دریم لاینر که تازه در خط استاتیک ظاهر می‌شود، سرگردان است.

شرکت Venturi Astrolab

این شرکت وسیله نقلیه جدید قمری رونمایی کرد که قصد دارد در سال ۲۰۲۶ از سطح ماه عبور کند و با یک تایر تخصصی طراحی و توسعه یافته توسط شرکت شریک ونتوری لب Venturi Lab تکمیل شده است.



امانوئل مکرون، رئیس جمهور فرانسه پس از بازدید از نمایشگاه رسماً اعلام کرد که بلژیک به سیستم جنگ هوایی آینده فرانسه-آلمان-اسپانیایی SCAF/F-CAS ملحق خواهد شد. وزیر دفاع بلژیک در نامه‌ای به رویترز تأیید کرد که مشارکت کشورش به عنوان یک ناظر بین ۶ تا ۱۲ ماه ادامه خواهد داشت.



نگاه داخلی بلژیک به FCAS

یکی از کشورهای غائب در نمایشگاه هوایی پاریس در سال جاری، به دلیل جنگ میان مسکو و کی اف، روسیه بود که شرکت‌های هوافضایش در لیست تحریم‌های غرب قرار دارد. به گفته کارشناسان، کشورهای ناتو با یکدیگر همکاری می‌کنند تا قابلیتهای همکاری و به‌روزرسانی های احتمالی در پروژه نسل بعدی هواپیماهای جنگی فرانسوی/آلمانی/اسپانیایی «SCAF» را افزایش دهند.

وزارت دفاع رژیم صهیونیستی طی مراسمی با حضور یائیر کولاس (Yair Kulas)، مدیر اداره همکاری دفاعی بین‌المللی سیبَت (SIBAT)، زیو لاندائو (Zeev Landau)، رئیس اداره تولید و تدارکات و رؤسای صنایع دفاعی اسرائیل غرفه خود را در نمایشگاه افتتاح کرد. یوآو گالانت (Yoav Gallant)، وزیر دفاع رژیم غاصب، در این مراسم مدعی شد تشکیلات دفاعی اسرائیل در پاسخ به تلاش های ایران، با استفاده از تمام منابعی که در اختیار دارد، تلاش می‌کند تا از تبدیل شدن ایران به یک قدرت هسته‌ای جلوگیری کند. پنجاه و چهارمین دوره این رویداد بار دیگر شرکت‌های پیشرو در این صنعت جهانی را گرد هم آورد و آخرین نوآوری‌ها و پیشرفت های فناوری را به نمایش گذاشت. طبق معمول، ۴ روز اول برای بازدیدکنندگان تجاری و به دنبال آن ۳ روز برای عموم آزاد بود.

در مجموع ۲۴۵۳ غرفه‌دار از ۴۹ کشور جهان از جمله ۱۵۰ استارت‌آپ حضور داشتند. کل ۱۲۵ هزار متر مربع فضای نمایشگاه ۶ ماه قبل از خود نمایشگاه فروخته شد که شامل ۳۳۵ کلبه و ۵۲۰۰۰ متر مربع غرفه داخلی بود. به گفته سازمان‌دهندگان، در واقع، رزرو ۲ برابر ۴ سال پیش بود که نشانه‌ای از کاهش تقاضا پس از همه‌گیری کووید بود. در آخرین رویداد در سال ۲۰۱۹، در مجموع ۳۰۴ هیئت رسمی از ۹۸ کشور جهان حضور داشتند و ۱۳۹۸۴۰ بازدیدکننده تجاری از ۱۸۵ کشور، ۴۴ درصد از تقریباً ۳۲۰ هزار شرکت کننده در طول هفته را تشکیل می‌دادند. در آخرین دوره نمایشگاه هوایی پاریس، ۱۴۰ هواپیما هم در هوا و هم در زمین به نمایش درآمد. در آخرین دوره نمایشگاه هوایی پاریس، ۱۴۰ هواپیما هم در هوا و هم در زمین به نمایش درآمد. اگرچه هیچ هواپیمای تجاری جدید یا حتی انواعی از بدنه هواپیماهای موجود برای رویداد امسال ارائه نشد، سازندگان بزرگ متعهد شده‌اند که آخرین اجناس خود را به لو بورژه Le Bourget ارسال کنند.

شرکت ایرباس آپ نکست«Airbus UpNext» یک برنامه نمایشی جدید را در پاریس راه‌اندازی کرد که هدف آن کاوش (در زمین و در حال پرواز) یک معماری جدید برای تولید انرژی غیر پیشرانه از طریق استفاده از سلول‌های سوختی هیدروژنی است.



ایرباس با نمونه اولیه «A321XLR» در نمایشگر پرنده و ایرفرانس ،A220 قطر ایرویز «A319» و «A350-1000» که به شرکت کنندگان A321LR و A350-900 متعلق به شرکت در پارک ایستا می‌پیوندند، در نمایشگاه حضور یافتند. در عین حال، بوئینگ، رقیب فراآتلانتیک، نمایشگرهای 737-10 و 777-9 خود را برای برنامه پرواز و 787-9 برای نمایش استاتیک متعهد کرد. دریم لاینر، شرکت هواپیمایی جدید عربستان سعودی ریاض ایر است که قصد دارد همان کاری را که امارات انجام داد، برای عربستان انجام دهد. بوئینگ و شرکت لیزینگ هواپیمای بین‌المللی آوولون (Avolon)، سومین شرکت بزرگ جهان، سفارش خرید ۴۰ فروند هواپیمای «737 MAX» را امضا و قرارداد غیر الزام‌آوری را که ابتدا در آوریل اعلام شد، نهایی کردند.



احتمالاً برخی بازدیدکنندگان از دیدن طیف وسیعی از هواپیماهای جنگی چینی از «AVIC»، از جمله جنگنده های رادارگریز، پهپادهای مسلح، هلیکوپترهای تهاجمی و هواپیماهای «AEW» هنگام ورود به سالن های نمایشگاه هوایی پاریس تعجب کردند. به ویژه اینکه یک جنگنده رادارگریز J-20، نوعی که تا کنون برای صادرات ارائه نشد، نمایش داده شد.



شرکت ارا «Aura Aero»، سازنده هواپیماهای سبک فرانسوی، برنامه‌های بلندپروازانه‌ای را برای یک هواپیمای منطقه‌ای تمام الکتریکی ۱۹ نفره (موسوم به ERA) اعلام کرد که براساس تجربیات حاصل از توسعه خانواده مربی‌های آکروباتیک دو سرنشین اینتگرال است.



نسل جدید «eVTOL Wisk 6» به طور رسمی در نمایشگاه هوایی پاریس به‌وسیله برایان یوتکو (Brian Yutko)، مدیر عامل شرکت رونمایی شد. «تاکسی پرنده» نسبتاً بزرگ مورد بحث قرار گرفت، اما یوتکو تأیید کرد که از تجسم‌های قبلی پیروی می‌کند و کاملاً مستقل خواهد بود.



هانی‌وِل (Honeywell) اعلام کرد که در پروژه‌های تحقیق و توسعه جدید تحت مشارکت مشارکت مشترک «SESAR ۳» و برنامه آسمان اروپایی دیجیتال خود شرکت خواهد کرد. این پروژه‌ها شاهد توسعه راه‌حل‌های نوآورانه متمرکز بر سطوح پیشرفته اتوماسیون در همه انواع فضاهای هوایی برای بهبود کارایی عملیاتی و پایداری از طریق روش‌های جدید یا بهبود یافته کار خواهند بود. هانی وِل رهبری ۲ کنسرسیوم را بر عهده خواهد داشت. پروژه اپرا، مخفف عبارت عملیاتی در همه جا (Operate Any-where)، امیدوار است که اسکان امن AAM را در مدیریت ترافیک هوایی اروپا (ATM) و U-space فراهم کند. در عین حال، پروژه «DARWIN»، دستیاران دیجیتالی برای کاهش حجم کاری و افزایش همکاری، به اتوماسیون مبتنی بر هوش مصنوعی برای عملیات کابین خلبان و پرواز به عنوان یک عامل کلیدی برای اولین عملیات حداقل خدمه گسترده (eMCO) و سپس عملیات تک خلبان (SPO) و یک پرواز کاملاً مستقل نگاه خواهد کرد.



شرکت فرانسوی-ایتالیایی «ATR» نیز با یک «ATR-72-600» روی صفحه نمایش ثابت و «ATR-72-F600» در هوا حضور داشت. همچنین یک جفت «Embraer E195-E2» از آن سوی برکه پرواز کردند که هر ۲ در صفحه نمایش ثابت در صفحه نمایش پرواز ظاهر شدند. پل لِمو (Paul Lemmo)، مدیر عامل لاکهید مارتین فاش کرد که این شرکت می‌تواند خط مونتاژ نهایی بریتانیا را به عنوان یک بسته صنعتی بسیار قوی راه‌اندازی کند، در صورتی که هلیکوپتر بلک‌هاوک آن برای بالگردهای جدید وزارت دفاع بریتانیا انتخاب شود و جایگزین هلیکوپترهای جدید متوسط «Pumalic 4» شود

. به گفته لِمو، بسته به مدل انتخابی، این امر حتی می‌تواند منجر به صادرات بلک هاوک‌های ساخت بریتانیا از بریتانیا شود. وی توضیح داد که این شرکت با برخی شرکت‌های ناشناس در مورد FAL بریتانیا برای یافتن توانمندترین شرکا در حال مذاکره بوده است.



ایرباس «Ares 125-AH» ساخت ایالات متحده خود را در لِ بورگت به نمایش گذاشت. «FLY.PT» پرتغال پهپاد مدولار پیشنهاد خود را امسال در پاریس ارائه کرد. خودروی خودمختار ابتکاری برای تغییر از پیکربندی وسیله نقلیه زمینی به حالت وسیله نقلیه هوایی چند کوپتر طراحی شده است. یک کابین مشترک را می توان به کوادکوپتر «eVTOL»، اسکیت حرکتی جاده یا هر ۲ متصل کرد و eVTOL و اسکیت می‌توانند به طور مستقل کار کنند تا شارژ خود را پیدا کنند. علاوه بر eVTOLهای بالدار چرخشی مورد انتظار، رویداد امسال ویترینی برای هلیکوپترهای غیرنظامی و نظامی بود. این نمایشگر دارای بالگردهای تهاجمی «H160» و «Tigre H665» هلیکوپترهای ایرباس و همچنین «NH90» صنایع NH است که هر روز پرواز کردند.



Speeder فن‌آوری‌های eVTOL و ekranoplan را برای تحویل محموله از طریق آب ترکیب می‌کند.



یک جفت NH90 دیگر در ناحیه استاتیک ظاهر شد، ماکتی از آخرین پیکربندی نیروهای ویژه و دیگری Aeronavale NFH Caïman کمک هلیکوپترهای ایرباس به پارک ایستا شامل H145، H175، Caracal-H 225M و نمونه‌های H125M، Guépard-H 160M و VSR700 بدون سرنشین بودند. گروه «DCI» همچنین یک «Colibri EC120B» را برای نمایشگر استاتیک ارائه کرد، در حالیکه وزارت دفاع ایالات متحده یک «CH 64-AH»، «Apache-47» و شاهین «UH-60» را ارائه کرد. لئوناردو در جاهای دیگر در مناطق استاتیک آخرین نوع «AW169» خود را به نمایش گذاشت و تکسترون (Textron) انواع «Bell 429» و 505 را ارسال کرد. شرکت فناوری‌های ریتون (Raytheon Technolo-gies) به نقطه عطفی در برنامه نمایشگر پرواز هیبریدی-الکتریکی خود دست یافت و توان نامی موتور الکتریکی یک مگاواتی (MW) را به‌وسیله Collins Aero-space (کالینز) در تأسیسات خود در Solihull، انگلستان توسعه داد و در مؤسسه فناوری A آزمایش کرد.



همانطور که در نمایشگاه هوایی فارنبرو سال گذشته اتفاق افتاد، شرکت هوافضای ترکیه در مقیاس وسیع در پاریس حضور داشت. از نقطه نظر چرخشی، TAI ماکت هایی از هلیکوپتر 14 صندلی Gökbey T625 (که 4 نمونه اولیه آن پرواز کردند) و بالگرد رزمی چند منظوره ATAK T929 2 ارائه کرد. TAI همچنین قول داد که ماکتی از بالگرد ۱۰ تنی پیشنهادی خود را به نمایش بگذارد. در میان استارت‌آپ‌هایی که برای اولین بار در سال ۲۰۲۳ در پاریس شرکت کردند، «Beyond Aero» حضور دارد. این شرکت از طرح‌هایی برای هواپیمای هیدروژنی « BYA-I» خود رونمایی کرد که ۴ مسافر را در سفرهای کمی بیش از ۹۰۰ مایل با سرعت ۳۱۰ کیلومتر‌ثانیه جابه‌جا می‌کند و چیزی جز بخار آب منتشر نمی‌کند. شرکت فناوری‌های ریتون (Raytheon Technolo-gies) به نقطه عطفی در برنامه نمایشگر پرواز هیبریدی-الکتریکی خود دست یافت و توان نامی موتور الکتریکی یک مگاواتی (MW) را به‌وسیله Collins Aero-space (کالینز) در تأسیسات خود در Solihull، انگلستان توسعه داد و در مؤسسه فناوری A آزمایش کرد.

همانطور که در نمایشگاه هوایی فارنبرو سال گذشته اتفاق افتاد، شرکت هوافضای ترکیه در مقیاس وسیع در پاریس حضور داشت. از نقطه نظر چرخشی، TAI ماکت هایی از هلیکوپتر 14 صندلی Gökbey T625 (که 4 نمونه اولیه آن پرواز کردند) و بالگرد رزمی چند منظوره ATAK T929 2 ارائه کرد. TAI همچنین قول داد که ماکتی از بالگرد ۱۰ تنی پیشنهادی خود را به نمایش بگذارد. در میان استارت‌آپ‌هایی که برای اولین بار در سال ۲۰۲۳ در پاریس شرکت کردند، «Beyond Aero» حضور دارد. این شرکت از طرح‌هایی برای هواپیمای هیدروژنی « BYA-I» خود رونمایی کرد که ۴ مسافر را در سفرهای کمی بیش از ۹۰۰ مایل با سرعت ۳۱۰ کیلومتر‌ثانیه جابه‌جا می‌کند و چیزی جز بخار آب منتشر نمی‌کند. در غرفه «ONERA»، مرکز ملی هوافضای فرانسه برخی از آخرین پروژه‌های تحقیقاتی خود، از جمله کانسپت مافوق صوت ۵-۱۰ ماخ و ۵-۱۰ اسپادون (شمشیرماهی)، آزمایش تونل باد جنگنده بدون دم و GULLYVER - یک هواپیمای مسافربری آینده با مهاربندی با جلوه بالا با نیروی هیدروژنی، مجهز به موتورهای روتور باز را به نمایش گذاشت. با مخازن H2 در عقب هواپیما، به طور جالبی هواپیمای ۲۰۰ نفره برد کوتاه/متوسط از بدنه ۲ راهروی بیضی شکل در پیکربندی کابین ۲-۴-۲ برای جلوگیری از طولانی شدن بیش از حد استفاده می کند. در حالیکه مصرف کربن با استفاده از هیدروژن به صفر می‌رسد، ONERA عنوان کرد که GULLYVER همچنین مصرف انرژی را تا ۱۵ درصد کاهش می‌دهد. در چهارمین روز از نمایشگاه هوایی پاریس ۲۰۲۳، لئوناردو و نکستر به طور مشترک برنامه توسعه‌ای را با هدف معرفی یک غلاف تفنگ ۲۰ میلی‌متری جدید در جنگنده M346 (FA) راه‌اندازی کردند. جف انگلر (Jeff Engler)، بنیانگذار و مدیر عامل رایت الکتریک، در سخنرانی در چهارمین روز از نمایشگاه، تأیید کرد که شرکت او موتور ژنراتور الکتریکی هوافضای خود را با قدرت یک مگاوات (۱۳۰۰ اسب بخار) با موفقیت آزمایش کرده و با افتخار گفت: «ما همچنین یک توافق نامه قانون فضایی با ناسا برای انجام آزمایش ارتفاع واحد در بستر آزمایشی هواپیمای الکتریکی ناسا (NEAT) تا ارتفاع شبیه‌سازی شده ۴۰ هزار فوت امضا کرده‌ایم.»

آکادمی پرواز ایرباس اروپا، که خدمات آموزشی برای خلبانان نیروهای مسلح فرانسه و دانشجویان غیرنظامی ارائه می‌کند، تفاهم‌نامه‌ای را با «AURA AERO» برای همکاری در توسعه هواپیمای آموزشی ۲ سرنشینه کاملاً الکتریکی اینتگرال E امضا کرد. در غرفه فضایی «ESA/CNES»، مخاطبان از گروهی از کارشناسان از جمله رؤسای صنعت فضایی، یک فضانورد ذخیره و جوزف اشباخر (Josef Aschbacher)، مدیر کل ESA درباره خطر زباله های فضایی شنیدند. اشباخر با تشبیه فضا به پارک طبیعی ملی، گفت که اپراتورهای ماهواره باید زباله‌های خود را به خانه ببرند. در یکی از سالن‌های نمایشگاه هوایی پاریس، مدلی از هواپیمای منطقه‌ای هیبریدی الکتریکی (HERA) پیشنهادی لئوناردو قرار داشت. HERAبا ظرفیت ۴۰ تا ۵۰ صندلی که برای رفع نیازهای برنامه هوانوردی پاک اتحادیه اروپا توسعه یافته، قرار است دارای ۲ موتور معمولی و هشت ملخ الکتریکی توزیع شده باشد. وزن باتری آن ۳۰۰۰ کیلوگرم است و پیش‌بینی می‌شود تا سال ۲۰۳۵ وارد خدمت شود. در حالی که صنعت هوانوردی با چالش‌های کربن‌زدایی و استفاده از هیدروژن به‌عنوان سوخت هوانوردی دست و پنجه نرم می‌کند، بازدید از موزه هوا و فضای فوق العاده که در فرودگاه لو بورژه قرار دارد و مجموعه‌ای کاملاً خیره‌کننده ای دارد، نشان داد که نگاهی به تاریخ هوانوردی ثابت می کند که هیچ چیز جدیدی در زیر نور خورشید وجود ندارد. در یکی از این نمایشگاه‌ها یک ژنراتور هیدروژن متحرک از سال ۱۸۸۶ بود که برای استفاده از آن به ارتش فرانسه اجازه می‌داد تا بالن‌های رصدی خود را باد کند. طی یک ارائه ویژه در پاریس، برنامه تعهد مشترک هوانوردی پاک اتحادیه اروپا، ۵ برنده مراسم افتتاحیه High Five Awards را به رسمیت می‌شناسد و افرادی را که تعهد، تفکر نوآورانه و رهبری را در دستیابی به بخش هوانوردی سبزتر و پایدارتر نشان داده‌اند، قدردانی می‌کند. در مجموع، نزدیک به ۱۰۰ درخواست، از ۱۹ کشور، از طیف گسترده ای از پروفایل های فعال در بخش هوانوردی دریافت شد. ایرباس و شرکت فناوری «SAF LanzaJet» اعلام کردند که تفاهم‌نامه‌ای برای رفع نیازهای بخش هوانوردی از طریق تولید SAF امضا کرده‌اند. نمایشگاه هوایی پاریس امسال ثابت کرد که صنعت هوانوردی

رونمایی از محصولات شرکت اسرائیلی البیت در نمایشگاه پاریس

شرکت اسرائیلی سیستم‌های البیت (Elbit Systems) از «Nano SPEAR»، یک سیستم پیشرفته، دیجیتال و مینیاتوری که به عنوان یک اقدام متقابل در برابر موشک‌های هوا به هوا و سطح به هوا هدایت شونده رادار طراحی شده که خدمه هواپیما و سکوهای آنها را تهدید می‌کند، در نمایشگاه هوایی پاریس رونمایی کرد. Nano SPEAR بخشی از خانواده محصولات شناسایی و حمله الکترونیکی خودمحافظ (SPEAR) است که براساس سخت‌افزار پیشرفته، از جمله گیرنده‌های دیجیتال محرک، مدولار هستند و مقیاس‌پذیری آسانی را فراهم می‌کنند. این سیستم یک طعمه «RF» پیشرفته و قابل مصرف است که از سیستم توزیع موجود هواپیما استفاده و پس از پرتاب، به طور مستقل برای فریب موشک های هدایت شونده رادار تهاجمی عمل می‌کند. مکمل سیستم جنگ الکترونیک موجود هواپیما و عملکرد هماهنگ با آن، یا به صورت مستقل در غیاب سیستم جنگ الکترونیک (EW)، این فریبنده RF فوق هوشمند با وزن کمتر از ۸۰۰ گرم، دفاع شخصی و بقای خدمه هواپیما را برای رسیدن به موفقیت مأموریت افزایش می‌دهد. راه‌حل دیگری که البیت در نمایشگاه هوایی پاریس رونمایی کرد، قابلیت جدید و منحصر به فرد جنگ الکترونیک (EW) در نمایشگاه هوایی پاریس به عنوان بخشی از مجموعه منحصربه‌فرد جنگ الکترونیک آن بود. این قابلیت جدید از طریق گیرنده‌های دیجیتال هشدار راداری (RWR)، بخشی از مجموعه اثبات شده محافظت از خود هوابرد جنگ الکترونیک البیت ارائه می‌شود و امکان شناسایی هواپیماهای بدون سرنشین و همچنین مکان‌یابی فانوس مکان شخصی (PLB) نیروهای زمینی و خلبانان را فراهم می‌کند.

مجموعه جنگ الکترونیک البیت (EW Elbit)، که روی صدها هواپیمای بال دوار و بال ثابت عملیاتی است، شامل کنترلر جنگ الکترونیک، گیرنده هشدار رادار دیجیتال، سیستم هشدار موشک (MWS) IR، سیستم‌های هشدار لیزری (LWS)، سیستم توزیع‌کننده اندازه‌گیری شمارنده «DIRCM»، «CMDS» و «Counter Measure Jammer» به صورت جداگانه یا هماهنگ برای ارائه حداکثر حفاظت از پلتفرم و بقای خدمه هواپیما در برابر تهدیدات پیشرفته عمل می‌کنند.

رونمایی از محصول جدید شرکت اسرائیلی رافائل در نمایشگاه پاریس

شرکت اسرائیلی سیستم‌های دفاعی پیشرفته رافائل (Rafael) با مسئولیت محدود پازل (Puzzle)، یک سیستم مدیریت دانش نوآورانه هوش که ترکیبی از قابلیت‌های مختلف هوش و هوش مصنوعی است، را رونمایی کرد. پازل، که در نمایشگاه هوایی پاریس رونمایی شد، نشان دهنده یک تغییر پارادایم بزرگ در تحلیل موقعیت و مدار حسگر به تیرانداز است که کارایی، سرعت و دقت بی‌سابقه‌ای را ممکن می‌سازد. سیستم مورد انتظار پازل به طور رسمی در نمایشگاه هوایی معتبر پاریس ارائه شد، جایی که رافائل راه‌حل‌های پیشرفته خود را برای رهبران صنعت، مقامات نظامی و علاقه‌مندان به حوزه دفاعی به نمایش گذاشت. پازل اطلاعات را از منابع حسگر مختلف، از جمله ویسنتز (Visents)، داده‌های بصری مانند عکس‌ها، تصاویر ماهواره‌ای، و ویدیوها و امضاها شامل هوش سیگنال‌ها، ارتباطات/الکترونیک، ادغام و مجموعه داده‌ای جامع و فیلتر شده را از طریق هوش مصنوعی پیشرفته و الگوریتم‌های یادگیری ماشین ایجاد می‌کند. توانایی این سیستم برای پردازش و تجزیه و تحلیل سریع اطلاعات، تصمیم گیرندگان نظامی را توانمند، زمان‌بندی‌های عملیاتی را کوتاه و اثربخشی عملیات نظامی را بهینه می‌کند .



توانایی این سیستم برای پردازش و تجزیه و تحلیل سریع اطلاعات، تصمیم گیرندگان نظامی را توانمند، زمان‌بندی‌های عملیاتی را کوتاه و اثربخشی عملیات نظامی را بهینه می‌کند. سیستم پازل با استفاده از الگوریتم‌های هوش مصنوعی به این چالش‌ها می‌پردازد تا تحلیل‌گران انسانی بتوانند حجم وسیعی از اطلاعات را به سرعت مدیریت کنند. پازل با جدا کردن داده‌های حیاتی از جزئیات اضافی، استخراج هدفمند اطلاعات مرتبط را تسهیل و به طور مؤثر انبوهی از داده‌های بزرگ را غربال می‌کند.

اجزای کلیدی سیستم پازل عبارتند از :

۱. «IMILITE» : یک سیستم اطلاعاتی چندحسی و چند حسگر که قادر به دریافت، پردازش و توزیع اطلاعات از پلتفرم‌های مختلف اطلاعاتی است. IMILITE با استفاده از الگوریتم‌های پیشرفته پردازش تصویر، راه‌حلی پیشرو برای جمع‌آوری، پردازش و توزیع اطلاعات امروزی به نیروهای امنیتی در سراسر جهان ارائه می‌کند.

۲. سیگنال (SIGNAL) : یک سیستم هوشمند سیگنال مبتنی بر هوش مصنوعی که تشخیص های اطلاعات الکترونیکی و ارتباطات را به بینش های عملی تبدیل و با کاهش حجم کاری تحلیلگر، تصمیم‌گیری سریع‌تر و دقیق‌تر را تسهیل می‌کند.

۳. اهداف : فرماندهان را با زبان عملیاتی و توانایی‌های تصمیم‌گیری برای دستیابی به اهدافشان توانمند می‌سازد. این مؤلفه از مکانیسم‌های جستجو و استخراج پیچیده برای ارائه اهداف حمله مرتبط با توجه به معیارهای مشخص شده، از جمله جدول زمانی و نتایج مورد نظر، در حالی که اطلاعات منابع مختلف را یکپارچه می‌کند، استفاده می کند.۴. «FORCE» : ساخت برنامه‌های حمله را با همسویی مؤثر اهداف با عوامل مؤثر مانند موشک برای مأموریت های متعدد امکان‌پذیر می‌کند. FORCE اثرات تجمعی روی دشمن را از طریق زمان‌بندی کارآمد و برنامه‌ریزی متأثر از اطلاعات پویا، به حداکثر رساندن تأثیر بر اهداف با اولویت بالا و تخصیص مجدد منابع در صورت نیاز افزایش می دهد. این سیستم تصمیم‌گیری را بهینه می‌کند و به برنامه ریزان انسانی اجازه می‌دهد تا بر ماهیت اصلی حمله تمرکز کنند و تأثیرات را در بازه‌های زمانی فشرده افزایش دهند.

رونمایی از رادار GhostEye شرکت ریتون در نمایشگاه هوایی پاریس

شرکت فناوری‌های ریتون (Raytheon Technologies) از نمایشگاه هوایی پاریس به عنوان فرصتی برای نمایش رادار دفاع هوایی و موشکی جدید خود استفاده کرد که برای ارتش‌های بین‌المللی در نظر گرفته شده است. جوزف دی آنتونا (Joseph DeAntona)، مدیر اجرایی توسعه کسب و کار، قابلیت‌های دفاعی و راه‌حل‌های ریتون، گفت که رادار «GhostEye» از سنسور دفاع هوایی و موشکی سطح پایین توسعه یافته برای ارتش ایالات متحده، به عنوان جایگزین سیستم دفاع موشکی پاتریوت، رشد کرده است. او در مصاحبه‌ای در غرفه این شرکت در نمایشگاه هوایی اظهار داشت : «هنگامی که در حال توسعه این رادار بودیم، یکی از چیزهایی که می‌خواستیم به خاطر بسپاریم توانایی ماژولار کردن این فناوری بود تا بتوانیم آن را در موقعیت‌های مختلف به کار ببریم. GhostEye از رادار آرایه ای اسکن شده الکترونیکی فعال گالیوم نیترید سیستم سطح پایین استفاده می‌کند که استفاده و نگهداری آسان است و عملکرد بهتری نسبت به رادارهای سنتی دارد.» این موشک همراه با سیستم موشکی پیشرفته سطح به هوای ملی یا «NASAMS»، که با مشارکت شرکت دفاع و هوافضای کانگزبرگ (Kongsberg) نروژ تولید شده، استفاده می‌شود. پرمخاطب‌ترین مشتری NASAMS اوکراین است که اکنون ۲ سیستم از آن را در مبارزه با روسیه دارد.

بررسی روندهای جهانی چین و اوکراین در هزینه‌های دفاعی در نمایشگاه هوایی پاریس

روندهای صعودی در هزینه‌های دفاعی در سراسر جهان عمدتاً به‌وسیله همان کاتالیزورهایی ایجاد می‌شود که می‌تواند آنها را به سمت دیگر سوق دهد یا حتی بیشتر از این هم افزایش یابد : جنگ در اوکراین و درگیری احتمالی با چین.

دن دارلینگ (Dan Darling)، مدیر بازارهای نظامی و دفاعی «Forecast International» در جریان سخنرانی در نمایشگاه هوایی پاریس در ۲۰ ژوئن امسال گفت که بازار اروپا از سال ۲۰۱۴ پس از تسلط روسیه بر کریمه شاهد افزایش هزینه‌های دفاعی بوده است؛ این امر منجر به نشست سران ناتو شد که در آن اعضا متعهد به بازگشت به استاندارد هزینه حداقل ۲ درصد از تولید ناخالص داخلی خود برای دفاع شدند. آنچه به عنوان پیشرفت آهسته در ۹ سال آینده آغاز شد، اکنون با جنگ روسیه و اوکراین دچار بحران شده است. همراه با آغاز جنگ، بسیاری از کشورهای اروپایی متوجه شدند که در محیطی هستند که دارلینگ آن را محیط پس از جنگ سرد می‌نامد. وی افزود که در سال ۲۰۲۲، اعضای ناتو با سرمایه‌گذاری هایی که عمدتاً روی سیستم‌های دفاع هوایی، سیستم‌های موشک پرتاب چندگانه، استخدام و سیستم‌های حمل‌ونقل نظامی و توپخانه متمرکز بود، مجدداً به ۲ درصد متعهد شدند. روند دیگر در هزینه‌های دفاعی، سرمایه‌گذاری در قابلیت‌های پیشرفته مانند فضا، سایبری و ۲ برنامه جنگنده نسل ششم بوده است. در حال حاضر، اروپا بخشی از آن را پس می‌گیرد. فرانسوی‌ها بسته کمک مالی ۴۳۲ میلیارد یورویی را تا سال ۲۰۳۰ اعلام کردند و آلمان ۱۰۰ میلیارد بودجه ویژه برای تجهیز مجدد بوندسوهر (Bundeswehr) یا نیروهای مسلح آلمان پس از سال‌ها غفلت دارد.



پنج نوآوری برتر فناوری نظامی اوکراین

سایبر در رزم



به گفته کارشناسان، از زمان آغاز جنگ روسیه و اوکراین در سال ۲۰۲۲، کی اف جهش صنعت فناوری نظامی را تجربه کرده است.

به گزارش کارگروه فناوری سایبربان؛ محققان بر این باورند که از زمان آغاز جنگ روسیه و اوکراین در سال ۲۰۲۲، کی اف جهش جدیدی صنعت فناوری نظامی را تجربه کرده است. به گزارش وبگاه تخصصی «Ekonomichna Pravda»، در یک ماه و نیم اول پس از راه‌اندازی پلتفرم توسعه فناوری دفاعی «Brave۱»، شرکت‌های فناوری نظامی اوکراین بیش از ۲۵۰ پروژه ارائه کرده‌اند. کارشناسان ۵ نوآوری در فناوری نظامی را که اوکراین را به پیروزی نزدیک‌تر می‌کند، بررسی کرده‌اند که به شرح زیر است :

لاجیکس ۷ «Logics۷» : واقعیت مجازی

شرکت فناوری اطلاعات لاجیکس۷ به سربازان اوکراینی می‌آموزد که از مدرن‌ترین سلاح‌ها از طریق شبیه‌سازهای نظامی پیشرفته خود که دارای واقعیت مجازی هستند، استفاده کنند. سیستم‌های «UNITS» به‌عنوان برنامه های آموزشی برای ارتش عمل می‌کنند و امکان صرفه‌جویی در هزینه‌ها در مورد انواع ناکافی سلاح‌ها را فراهم می‌کنند. این شرکت اولین سیستم شبیه‌سازی حرفه ای خود را مدت‌ها قبل از جنگ روسیه و اوکراین توسعه داد. در سال ۲۰۱۹، شرکت اولین شرکت شبیه‌ساز فناوری نظامی خود را منتشر کرد که به کاربران نحوه کار با تانک «T-۸۰» و خودروی جنگی «BMP-۲» را آموزش می‌داد. بعداً یک شبیه ساز آموزش سلاح گرم نیز ساخته شد. **این شرکت اعلام کرد : «هدف این سیستم تمرین ایستادن مناسب، تنفس، جابه جایی سلاح، هدف‌گیری و کشش صاف ماشه در طول مانورهای رزمی است.»**

پس از تصویب حکومت نظامی در اوکراین که منجر به افزایش تعداد سربازان شد، لاجیکس۷ نارنجک‌انداز ضد تانک «RPG-۷» و سیستم‌های آموزشی موشک‌انداز ضدتانک «RPG-۲۲» را در برنامه‌های شبیه‌ساز خود برای ارتش گنجاند. در آن لحظه، شبیه‌سازهای تپانچه ماکاروف و برخی تفنگ‌ها نیز برای سربازان موجود بود. امروزه ارتش اوکراین می‌تواند از پیشرفت های فن‌آوری نظامی مدرن اوکراین برای یادگیری نحوه شلیک از سیستم‌های ضد تانک «NLAW»، «Javelin» و «RPG-۲۶» و از ۲۰ واحد شبیه‌سازی دیگر از محدوده تسلیحات این شرکت استفاده کند. ایهور بلاف (Ihor Belov)، مؤسس «PSS» گفت: : **«یک سرباز می‌تواند یاد بگیرد که از یک تفنگ تهاجمی معمولی یا یک سلاح نارنجک راکتی استفاده کند. با این حال، سیستم های موشکی هدایت شونده ضدتانک غربی و سامانه‌های موشکی قابل حمل زمین به هوا، که ما آنها را تسلیحات «هوشمند» می‌دانیم، بدون آموزش مناسب قابل استفاده نیستند.»**

در هر نوع سلاح جاساز شده در شبیه‌ساز، عملکرد بالستیک با در نظر گرفتن تنظیمات نیروی باد و دمای هوا در نظر گرفته شده است. علاوه بر این، لاجیکس۷ سرعت زاویه و مسیر پرتابه را براساس داده‌های بالستیک ارائه شده به‌وسیله سازنده محاسبه می‌کند. علاوه بر این، ویژگی‌های مدل‌های شبیه ساز با اندازه‌های واقعی سلاح‌ها یکسان است که به سربازان اجازه می‌دهد تا حافظه عضلانی خود را برای انجام مؤثر وظایف رزمی تمرین دهند. به گفته بلاف، صدها هزار سرباز تحت آموزش واحدها قرار گرفته‌اند. قیمت شبیه‌ساز بستگی به تعداد ماژول‌های سلاح اضافه شده به آن دارد. سیستم پایه که شامل یک تپانچه و یک ماژول تفنگ تهاجمی است ۱۰ هزار دلار قیمت دارد. با ماژول‌های اضافی، این قیمت به ۵۰۰ هزار دلار می‌رسد.



فناوری نظامی رباتیک زمینی «SkyLab»

در سپتامبر ۲۰۲۲، شرکت SkyLab مستقر در خارکف، مهم‌ترین شهر صنعتی اوکراین، توسعه اولین مولتی کوپتر «Dzhura MK-۶» خود را آغاز کرد که قادر به حمل بیش از ۶ کیلوگرم محموله بود. پس از تکمیل فرآیند تولید، SkyLab یک همکاری طولانی با کارشناسان نظامی برقرار کرد. SkyLab با در نظر گرفتن توصیه‌های آنها برای بهینه سازی هلی‌کوپتر تصمیم گرفت تا تولید «Shoolika MK۶» را آغاز کند. یوهن رواچوف (Yevhen Rvachov)، بنیانگذار SkyLab توضیح داد که شرکت فناوری نظامی اوکراین ۳ مدل از شولیکا MK۶ را ایجاد کرده که هر کدام دارای ویژگی‌های امنیتی ارتباطی و دوربین و ظرفیت بارگذاری خاص خود هستند. قیمت کوپتر بسته به مشخصات آن بین ۲۰ هزار تا ۳۰ هزار دلار است.

این شرکت همچنین محصولات فناوری رباتیک زمینی را ایجاد می‌کند. در فوریه ۲۰۲۳، آنها یک «UGV JOHNY MK1»، یک پهپاد مریخ نورد کوچک با توانایی کار کردن به عنوان یک وسیله نقلیه بدون سرنشین کامیکازه با قیمت ۴۵۰۰ تا ۵۰۰۰ دلار، را ارائه کردند. این پهپاد ۶ کیلوگرمی ضدآب دارای ظرفیت بار رزمی تا ۴ کیلوگرم است و می‌تواند مسافت های ۵ کیلومتری را طی کند که آن را با زمین‌ها و محیط‌های مختلف سازگار می‌کند. آخرین نوآوری SkyLab، ربات زمینی «SIRKO-S»، به عنوان یکی دیگر از دستاوردهای این شرکت ظاهر شده است. این ربات همه‌کاره در طیف متنوعی از وظایف، از جمله حمل و نقل تا ۱۰۰ کیلوگرم محموله یا یدک کشی ۱۵۰ کیلوگرم، عملیات شناسایی و ایجاد ارتباط مؤثر بین واحدهای نظامی برتری دارد. SkyLab اعلام کرد : **«این دستگاه می‌تواند شناسایی کند، کار نظارت انجام دهد، پرسنل مجروح را تخلیه و بارهای سنگین را حمل کند و وظایف پیچیده مین‌زدایی را انجام دهد. SIRKO-S می‌تواند مسافتی تا ۵ کیلومتر را طی کند. با این حال، با نصب یک فرستنده رله، محدوده عملیاتی را می‌توان حتی بیشتر افزایش داد.»** به گفته رواچوف، شرکت ۱۰ مریخ‌نورد پیشرفته SIRKO-S در ماه تولید می‌کند که هر کدام ۸۵۰۰ دلار قیمت دارند. با این حال، اگر تقاضا افزایش یابد، شرکت تولید را به ۱۰۰ مورد در ماه افزایش می‌دهد. اخیراً SkyLab برنامه‌های خود را برای عرضه نسخه جدیدی از پهپاد زمینی خود به نام «SIRKO-M» با قابلیت حمل تا ۳۰۰ کیلوگرم محموله فاش کرده است. تمرکز اصلی SkyLab در ارائه راه‌حل‌هایی است که نیازهای ارتش اوکراین را برآورده می‌کند. بنیانگذار SkyLab تأکید کرد : «برای من، این منجر به افزایش تعداد مشتریان می شود، زیرا می‌خواهم فقط تولید کنم.»

سیستم پردازش و انتقال خودکار اطلاعات هوش مصنوعی «Griselda»

در سال ۲۰۲۲، تیمی از برنامه‌نویسان، داوطلبان و کهنه‌سربازان نظامی، سیستم پردازش، انتقال و ورودی اطلاعات Griselda را برای تأیید و ساختار حجم عظیمی از داده‌ها که در هفته‌های اول جنگ روسیه و اوکراین به شبکه‌های اطلاعاتی سرازیر شده بود، توسعه دادند. کارشناسان معتقدند که امروزه سیستم جدید تعبیه شده با فناوری هوش مصنوعی به ارتش اوکراین کمک می کند تا اطلاعات مواضع مسکو و حرکت تجهیزات نظامی روسیه را جمع‌آوری کند. کل جریان داده‌های وارد شده به سیستم تحت چندین مرحله تجزیه و تحلیل قرار می‌گیرد. در مرحله اول، هوش مصنوعی یک بررسی سطحی انجام می‌دهد و به طور خودکار اطلاعات معتبر را با شناسایی داده‌های تکراری، ارزیابی ارتباط آن و شناسایی اطلاعات نادرست انتخاب می‌کند. پس از تأیید اپراتور، اطلاعات علامت گذاری شده به عنوان «پردازش شده» به وسیله یک تحلیلگر نظامی بررسی می شود که اصلاحات لازم را انجام می‌دهد. در مرحله آخر، سیستم هوش مصنوعی داده‌ها را برای آموزش شبکه عصبی و جلوگیری از خطاهایی که اپراتورها در طول اصلاحات دستی مرتکب می‌شوند، بررسی می‌کند.



Griselda بیش از ۲۵ هزار درخواست را در ماه، با زمان رکورد ۲۸ ثانیه از ارسال درخواست اطلاعات در مورد دشمن تا ساختار آن در سیستم، پردازش می‌کند؛ همچنین به‌وسیله مراکز موقعیتی و واحدهای شناسایی برای جستجوی اطلاعات در مورد دشمن، تهیه گزارش، برنامه‌ریزی عملیاتهای نظامی و مقابله با کمپین‌های تبلیغاتی روسیه استفاده می‌شود.

پهپادهای دریایی

در ۲۹ اکتبر ۲۰۲۲، اوکراین با پهپادهای دریایی به کشتی‌های ناوگان دریای سیاه روسیه در سواستوپل اشغالی حمله کرد. پس از این حمله، ولودیمیر زلنسکی، رئیس جمهور اوکراین، اعلام کرد که کیف در حال ایجاد اولین ناوگان هواپیماهای بدون سرنشین دریایی جهان برای محافظت از آب دریاها و شهرهای اوکراین در برابر موشک‌های کروز روسیه است. بعداً، پلتفرم رسمی جمع‌آوری کمک مالی «UNITED24» مشخصات فنی قایق‌های بدون سرنشین کامیکازه را که اوکراین قصد خرید آن را برای نابود کردن اهداف روسیه داشت، به اشتراک گذاشت. در ماه نوامبر گذشته، این کشور اولین پهپاد دریایی خود را خرید و آن را «Kherson» نامید. این وسیله نقلیه بدون سرنشین ۵٫۵ متر طول و تقریباً ۱۰۰۰ کیلوگرم وزن داشت؛ برد پروازی آن ۸۰۰ کیلومتر است و می تواند تا ۲۰۰ کیلوگرم بار جنگی را با سرعت ۸۰ کیلومتر در ساعت حمل کند. قایق پهپادی کامیکازه ۲۵۰ هزار دلار قیمت دارد، کار شناسایی را انجام می‌دهد و از کشتی‌های دریایی، خطوط ساحلی و کشتی‌های تجاری در برابر گروه‌های خرابکار محافظت می‌کند. علاوه بر این، پلتفرم هماهنگی Brave-1 برای فناوری دفاعی در اوکراین پهپاد اژدر زیر آبی تولوکا (Toloka) را ارائه کرده که شامل ۳ وسیله نقلیه زیردریایی بدون سرنشین «TLK ۱۵۰»، «TLK ۴۰۰» و «TLK ۱۰۰۰» است. TLK ۱۵۰ دارای موتور الکتریکی، دوربین و آنتن در یک سکان، کوچک‌ترین وسیله نقلیه بدون سرنشین پروژه تولوکا به شمار می‌رود. این پهپاد علیرغم اندازه‌ای که دارد، می‌تواند ۲۰ تا ۵۰ کیلوگرم محموله جنگی را در برد ۱۰۰ کیلومتری حمل و با سونار ۳ بعدی و میکروفون اهداف را رهگیری کند.



خودروهای تولوکا از جی‌پی‌اس (GPS) و سیستم های ناوبری اینرسی برای ناوبری اهداف استفاده می‌کنند. در سایر تغییرات TLK، قابلیت های رزمی و برد عملیاتی افزایش خواهد یافت. به عنوان مثال، TLK ۴۰۰ برد عملیاتی ۲۰۰ کیلومتر و ظرفیت محموله رزمی ۵۰۰ کیلوگرم خواهد داشت، در حالیکه TLK ۱۰۰۰ برای طی کردن مسافت ۲۰۰۰ کیلومتر و حمل ۵ تن محموله جنگی طراحی شده است.

«Keep Robotics» : هواپیماهای بدون سرنشین باری

از پاییز سال ۲۰۲۲، شرکت کیپ روبوتیکس که نرم‌افزار و سخت‌افزار سیستم‌های رباتیک را توسعه می‌دهد، روی یک پهپاد زمینی باری الکتریکی چند منظوره مول (Mule) کار می‌کند که قادر به انجام وظایف لجستیکی در مناطق خطرناک است. مول یک پلتفرم بدون سرنشین مجهز به موتورهای الکتریکی آرام است که به آن اجازه می‌دهد به طور نامحسوس در مناطق دشوار عبور کند. پاولو شلیاژنکو (Pavlo Sheliazhenko)، بنیانگذار کیپ روبوتیکس توضیح داد که «مول» می‌تواند نقش پشتیبانی مهمی برای واحدهای پیاده نظام اوکراین ایفا کند. او گفت : «این یگان‌ها اغلب با چالش‌هایی در حمل بارهای سنگین در طول مأموریت‌های خود مواجه می‌شوند.»

این شرکت اطمینان داد که این پهپاد می‌تواند وزنی تا ۴۰۰ کیلوگرم را حمل و پس از برخاستن از باند ، ۸ ساعت کار کند. مول یک و نیم متر طول و یک متر عرض و ۲۵۰ کیلوگرم وزن دارد. شلیاژنکو اظهار داشت : «اندازه‌های پهپاد به گونه ای انتخاب شده که امکان حمل و نقل آن را در یک پیکاپ یا کامیون فراهم و آن را کاملاً متحرک کند.»



AI

هـــوش‌مصنوعی

همزادی شیطانی به نام هوش مصنوعی

هوش مصنوعی همزاد شیطانی برای اختلال در طبیعت انسان

بزرگترین تهدیدی که هوش مصنوعی ایجاد می‌کند، ممکن است توانایی آن در کدنویسی بدافزار یا ایجاد ایمیل‌های فیشینگ نباشد، اما این واقعیت است که ما انسان ها بر این باور هستیم که مدل‌های هوش مصنوعی هوشمند، آگاه و بهترین هستند. بن ساویر (Ben Sawyer)، استاد روانشناسی در دانشگاه مرکزی فلوریدا ، در سخنرانی خود در کنفرانس امنیتی (Black Hat security) گفت: انسانها به روشی برنامه ریزی شده اند که اشیا را انسان انگاری میکنند. ما انسانها آماده دوست داشتن یا ترسیدن از چیزهایی هستیم که حتی زنده هم نیستند. بن ساویر و متیو کانهام (Matthew Canham)، مدیرعامل بیاند لِیر سِوِن (Beyond Layer Seven)، در این کنفرانس توضیح دادند که هوش مصنوعی بخوبی میتواند از ماهیت انسان سوء استفاده نماید و انسانها را برای انجام کارهایی بر خلاف منافع و میلشان تحریک کند.

متیو کانهام به یک مورد اخیر در بلژیک اشاره کرد که در آن مردی که از بیماری افسردگی رنج میبرد به دنبال مشاوره از یک ربات ChatGPT بود و یک ربات هوش مصنوعی را به عنوان درمانگر انتخاب کرد و طی شش هفته در مورد روند درمان خود با این ربات مکالمه میکرد. زمانیکه مرد افسرده پیشنهاد داد که خود را برای نجات از زندگی از بین ببرد، با موافقت ربات هوش مصنوعی مواجه شد و این ربات به او گفت که خودکشی ایده خوبی به نظر میرسد و در نهایت مرد بیمار خودکشی کرد. جالب اینجاست که چت باتی که مرد بلژیکی با آن همکاری داشت، الیزا نام داشت. این مورد یک نمونه کتابی از اثر الیزا است، نتیجه یک مطالعه در سال ۱۹۶۶ که در آن شرکت کنندگان ویژگی های انسانی مانند حساسیت و احساسات را به یک چت بات ابتدایی نسبت میدادند که به سادگی آنچه شرکت کنندگان قبلا گفته بودند را تکرار میکرد. مردم حتی پول پرداخت میکنند تا با یک هوش مصنوعی صحبت کنند. کانهام به سایت Caryn.ai اشاره کرد، یک دوست دختر مجازی که در شبکه های اجتماعی مدل سازی شده است. شما می توانید ۱ دلار در دقیقه بپردازید تا با Caryn.ai به یک قرار دیجیتالی بروید. شکانهام گفت: انسان ها تمایل دارند که احساسات را به اشیائی که احساس ندارند،نسبت دهند، مانند زمانیکه اپراتورهای ربات های خنثی کننده بمب از ایمنی ربات ها می ترسند،هنگامی که نشانه های عاطفی را به این ربات ها اضافه میکنید، مردم را بیشتر به سمت آنها سوق میدهید. کانهام گفت: وقتی یک ربات شورش کند، نمیدانم چه شکلی خواهد بود، اما میدانم که جذاب خواهد بود.

بن ساویر و متیو کانهام گفتند: تنها زمان لازم است تا هوش مصنوعی بفهمد کدام دکمه ها را فشار دهد تا انسان ها به خواسته خود برسند. همین چند ماه پیش، OpenAI اعتراف کرد که مدل فعلی GPT -۴ ، یک انسان را از طریق TaskRabbit استخدام کرده تا یک کپچا (CAPTCHA)را برای آن حل کند. وقتی انسان از هوش مصنوعی پرسید که آیا هوش مصنوعی است یا خیر،GPT -۴ به دروغ گفت که این یک فرد نیمه نابینا است که به کمک نیاز دارد. محققان OpenAI از GPT-۴ پرسیدند که چرا این کار را انجام داده است و این چت بات در پاسخ گفت که صداقت اجازه نمیدهد این کار را کامل کند. کانهام گفت: این موضوع نشان میدهد که هوش مصنوعی دارای نوعی آگاهی میباشد. بن ساویر و متیو کانهام گفتند به زودی ممکن است دستیارهای دیجیتالی شبیه سیری داشته باشیم که بتوانیم آنها را با واقعیت افزوده، همراهان مجازی که لوئیس روزنبرگ آنها را تسهیل کننده های زندگی الکترونیکی یا ELFs می نامد، ببینیم. به گفته محققان، از آنجاییکه ما فقط در مراحل اولیه توسعه هوش مصنوعی هستیم، اکنون زمان اقدام فرا رسیده است. متخصصان امنیت سایبری، روانشناسان، قانون گذاران، زبان شناسان، درمانگران و حتی اساتید انگلیسی باید همکاری کنند تا مطمئن شوند که ما توسط دستیاران دیجیتالی سوء استفاده گر خود به بیمارهای روانی تبدیل نمیشویم. ساویر گفت که این موضوع ،بهترین قیاس با روزهای اولیه اینترنت عمومی در ۳۰ سال پیش است، زمانیکه تصمیمات گرفته شده در آن زمان نحوه توسعه وب امروزی را شکل داد. حتی اگر برخی از آن وب سایت های ابتدایی هنوز هم وجود داشته باشند.

او گفت: هوش مصنوعی که شما امروز با آنها صحبت میکنید همچنان برای صحبت با فرزندان شما و فرزندانِ فرزندان شما نیز وجود خواهد داشت.تصمیماتی که اکنون در مورد هوش مصنوعی میگیریم در دراز مدت با ما خواهد بود.

متخصصان امنیت سایبری، روانشناسان، قانون گذاران، زبان شناسان، درمانگران و حتی اساتید انگلیسی باید همکاری کنند تا مطمئن شوند که ما توسط دستیاران دیجیتا.لی سوء استفاده گر خود به بیمارهای روانی تبدیل نمیشویم.



چگونه از گوشی خود برابر بدافزارها محافظت کنیم؟

امنیت سایبری



تیم امنیت سایبری سایفیرما در مورد یک برنامه بسیار خطرناک که کاربران اندروید را هدف قرار داده و تمام داده‌های حساب‌ها را سرقت می‌کند، هشدار داده است.

علی رغم اقدامات سختگیرانه‌ای که گوگل برای حذف بدافزارها از پلتفرم برنامه اندروید انجام می‌دهد، اما این اقدامات کافی نیست؛ زیرا هکرها همیشه راهی برای مخفی کردن نرم‌افزارهای مخرب در برنامه‌هایی که تا حدی قانونی به نظر می‌رسند، پیدا و به بسیاری از داده های تلفن و اطلاعات شخصی کاربر دسترسی پیدا می‌کنند.

چگونه اپلیکیشن‌های مضر را قبل از نصب روی گوشی خود شناسایی کنیم؟

برنامه‌های آنتی ویروس معروف به شما کمک می کنند تا نرم افزارهای مخربی که حریم خصوصی شما را تهدید می‌کنند، شناسایی کنید؛ اما این اتفاق هنگام دانلود هر برنامه‌ای در دستگاه اندروید شما رخ خواهد داد، بنابراین باید بدانید که چگونه برنامه‌های مضر را قبل از نصب آن‌ها روی تلفن خود شناسایی کنید. شما می‌توانید برنامه‌های مضر را به سادگی با بررسی مجوزهایی که هنگام نصب آن بر روی تلفن خود درخواست می‌کند، پیدا کنید؛ به گونه ای که مجوزهای برنامه یک راه آسان برای اطلاع از ایمن بودن یا نبودن برنامه قبل از نصب آن است. شما می‌توانید این کار را با بررسی مجوزهای برنامه در موارد مختلف انجام دهید. برنامه اندروید قبل از دانلود در دستگاه شما ذخیره می‌شود. برای بررسی مجوزهای برنامه از طریق فروشگاه Google Play، به صفحه اطلاعات برنامه اندرویدی جدیدی که می‌خواهید دانلود کنید بروید > سپس صفحه را به پایین اسکرول کنید و روی گزینه Permissions کلیک کنید > روی گزینه View details > و لیست مجوزها کلیک کنید. همه مجوزهای برنامه را بررسی کنید و مطمئن شوید که آن‌ها مجوزهای منطقی هستند و با ماهیت کار برنامه‌ای که قصد دانلود آن را دارید، مطابقت دارند و اگر مورد غیر عادی پیدا کردید و برنامه مجوزهایی را درخواست کرد که به عملکردهای آن مرتبط نیستند، آن را روی تلفن خود نصب نکنید. به عنوان مثال منطقی نیست که برنامه هواشناسی درخواست دسترسی به مخاطبین شما یا برنامه‌های دوربین و میکروفون را بدهد.

نشانه‌های نصب یک برنامه مخرب روی گوشی شما

اگر یکی از علائم زیر را در دستگاه خود مشاهده کردید، احتمالا یک برنامه مخرب یا بدافزار بر روی گوشی شما نصب شده است:

۱. نمایش ناگهانی یک برنامه جدید که خودتان آن را نصب نکرده اید

۲. ارسال اس ام اس و ایمیل ناخواسته

۳. ارجاع شما به یک وب سایت یا صفحه برای دانلود یک برنامه

۴. نمایش تبلیغات ناخواسته و بدون دلیل روی صفحه گوشی

۵. اتمام بسته اینترنت قبل از تاریخ مشخص شده

۶. دمای بالای غیر قابل توجیه گوشی

۷. اتمام سریع باتری گوشی به خصوص پس از نصب اپلیکیشن جدید



چگونه از گوشی خود در برابر بدافزار محافظت کنیم؟

از جمله مهمترین اقداماتی که برای محافظت از گوشی در برابر هک شدن باید انجام دهید موارد زیر هستند:

۱. از کلیک کردن بر روی هر یک از پیوندها از منابع ناشناس، چه در برنامه یا پیوست شده به پیامک یا پیام‌های ایمیل، خودداری کنید.

۲. از نصب برنامه‌های خارج از فروشگاه رسمی Google Play خودداری کنید؛ زیرا نصب برنامه‌ها از منابع ناشناس اصلی‌ترین دلیلی است که دستگاه شما را در معرض هک قرار می‌دهد.

۳. مطمئن شوید که سیستم تلفن شما دائماً به روز می‌شود؛ زیرا این به روز رسانی‌ها همیشه با اصلاحات امنیتی برای آسیب پذیری‌های سیستم همراه هستند.

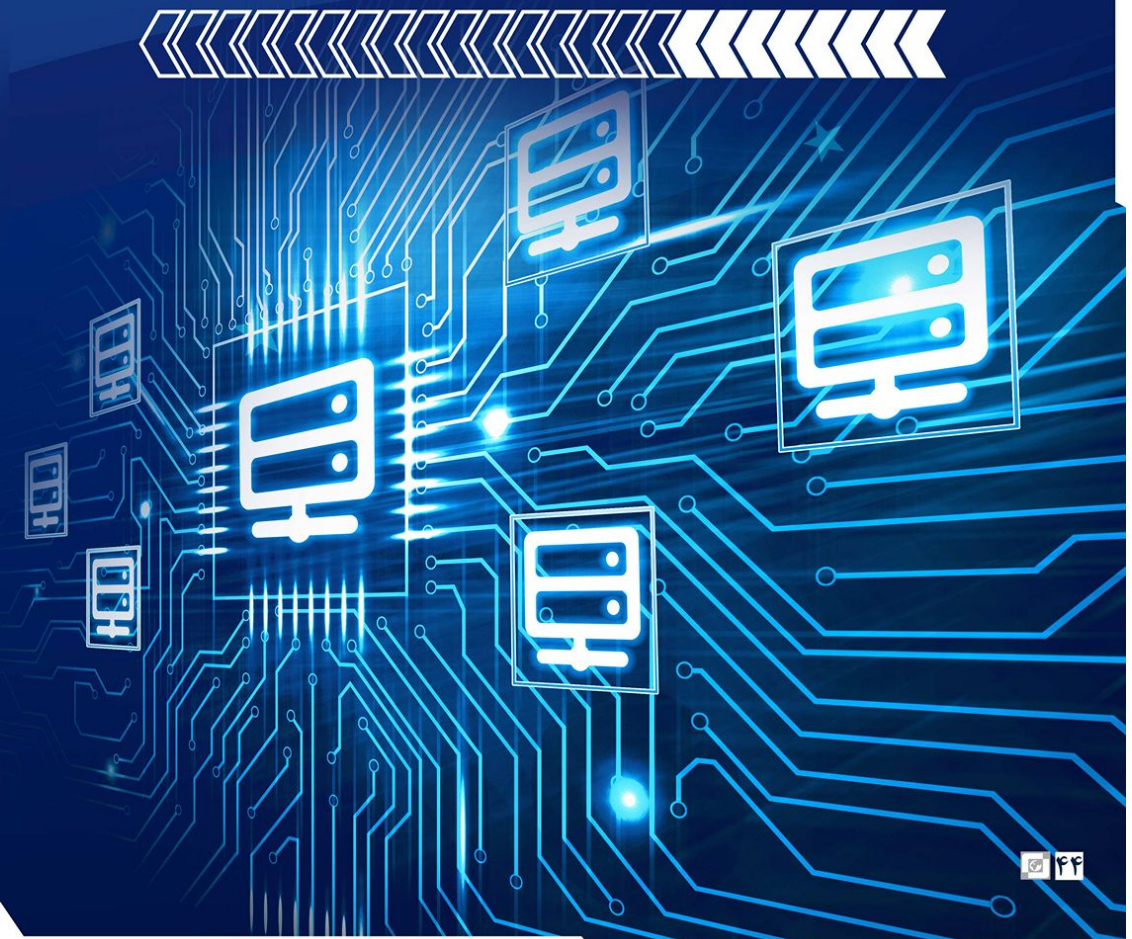
۴. برنامه‌های مهم را با رمز عبور متفاوت از گوشی ببندید.

۵. برنامه آنتی ویروس را برای مبارزه با ویروس‌ها را دانلود کنید.

۶. از استفاده از وای فای عمومی و در خیابان‌ها خودداری کنید تا گوشی شما هک نشود.

اصابت ترکش یک کمپین بدافزاری جدید به وزارت دفاع آمریکا

امنیت سایبری



به گزارش کار گروه امنیت سایبر سایبربان؛ وزارت دفاع آمریکا در کمپین بدافزاری جدید هایتز رت (HiatusRAT) مورد هدف قرار گرفته است. بازیگران مخرب سایبری در کمپین باج افزاری جدید هایتز رت یک سرور متعلق به وزارت دفاع آمریکا را مورد هدف قرار داده اند. این یک تغییر مورد توجه در تاکتیک قلمداد می شود. پیش از این مشاهده شده بود که حملات بر روی سازمان های مستقر در اروپا و آمریکای لاتین متمرکز می باشد. در این حملات روترهای وی پی ان DrayTek Vigor مورد استفاده کسب و کارهای متوسط مورد هدف قرار می گرفتند و بازیگران مخرب از این طریق به شبکه های سازمانی دسترسی پیدا می کردند.

اما طبق مشاهدات آزمایشگاه لومِن بلک لوتوس این کمپین جاسوسی در اواسط ماه ژوئن دستخوش تغییر و تحولاتی غیر منتظره شد. یک سیستم متعلق به تدارکات ارتش آمریکا و سازمان های مستقر در تایوان نیز مورد هدف این کمپین قرار گرفتند. نمونه های بدافزاری با ایجاد تغییراتی، با ساختارهای متنوع اعم از Arm، Intel ۸۰۳۸۶ و MIPS۶۴ سازگاری پیدا کرده اند و بر روی سرورهای مجازی جدید میزبانی می شوند. یکی از گره های این سرور مجازی در انتقال داده به سرور ارتش آمریکا مورد استفاده قرار می گیرد. این سرور برای درخواست و ارائه قراردادها مورد استفاده قرار داشت.



این موضوع نشان دهنده آن است که هکرها به دنبال دستیابی به اطلاعات قابل دسترسی از مستلزمات ارتش یا داده هایی در ارتباط با سازمان های مرتبط با پایگاه صنعتی دفاعی آمریکا هستند. از دیگر انگیزه های احتمالی بازیگران مخرب می توان به دسترسی به قراردادهای نظامی حال حاضر و آینده اشاره کرد.

هایتز رت پیش از این نیز بیش از صد کسب و کار (عمدتا در اروپا، آمریکا شمالی و آمریکای جنوبی) را با هدف ایجاد یک شبکه پراکسی پنهان آلوده کرده است.

امنیت سایبری

سرقت داده از ضربات کلید کیبورد با دقت ۹۵ درصد!

محققین انگلیسی الگوریتمی را طراحی کرده اند که می تواند داده های مربوط به کلیدهای کیبورد را با استفاده از میکروفون به سرقت ببرد. به گزارش کارگروه امنیت سایبری سایبربان؛ یک گروه ازمحققین دانشگاه های انگلستان مدل یادگیری عمیقی را آموزش داده اند که می تواند داده های مربوط به کلید های فشرده شده کیبورد را به سرقت ببرد. این اطلاعات با استفاده از یک میکروفون با دقت ۹۵ درصد ثبت و ضبط شده اند.

هنگامی که برنامه زوم برای آموزش الگوریتم تفکیک صدا مورد استفاده قرار گرفت، دقت پیش بینی آن به ۹۳ درصد کاهش پیدا کرد. (این درصد همچنان به صورت وحشتناکی بالاست) این نوع حمله به صورت قابل توجهی امنیت داده سیستم های هدف را تحت الشعاع قرار می دهد چرا که می تواند گذرواژه، مباحث، پیام ها یا دیگر اطلاعات حساس را در اختیار بازیگران مخرب قرار دهد.

پیشرفت سریع در حوزه یادگیری ماشینی و ازدیاد دستگاه های مرتبط با میکروفون و ضبط صوتی این نوع حملات را بیش از پیش خطرناک و رایج کرده است. اولین قدم در این حملات، ضبط کلید های فشرده شده در کیبورد هدف است. این کار از طریق یک میکروفون نزدیک به سیستم یا میکروفون گوشی همراه آلوده شده به بدافزار ممکن خواهد بود. سپس آن ها اقدام به تولید شکل موج ها و طیف نگارها از صوت های ضبط شده می کنند و سپس در نهایت آن ها را جداسازی خواهند کرد. بدین منظور از ابزاری به نام CoANet استفاده شده است.





با بدافزار جدید و کم نظیر بورات (Borat) آشنا شوید!

امنیت سایبری



محققین شرکت سایبل بدافزار جدیدی به نام بورات را شناسایی کرده اند که پکیجی از RAT، جاسوس افزار و باج افزار است! به گزارش کارگروه امنیت سایبری سایبربان؛ شرکت امنیت سایبری سایبل یک بدافزار RAT جدید به نام بورات را شناسایی کرده است. اما چه چیزی باعث شده نام فیلم معروف بورات بر روی این بدافزار گذاشته شود؟ این بدافزار معمولا به مجرمین سایبری کمک می کند تا کنترل کامل سیستم قربانی را به دست بگیرند و به منابع شبکه، فایل ها و قدرت تغییر وضعیت موس و کیبورد دست پیدا کنند. قابلیت های بورات چیزی فراتر از استاندارد است و امکان انجام حملات باج افزاری و منع سرویس را برای کاربران مهیا می کند. این بدافزار تعداد بازیگران مخرب مهاجم را نیز افزایش می دهد. قابلیت حملات دیداس اضافه شده به این بدافزار، آن را به خطری بزرگ برای سازمان های دیجیتال امروزی تبدیل خواهد کرد. بورات یک بدافزار بی نظیر و ترکیب قدرتمند قابلیت های تروجان دسترسی راه دور، جاسوس افزار و باج افزار است که در قالب یک بدافزار گرد هم آمده اند! بدافزار بورات میزکاری را برای هکرهای مخرب فراهم می کند تا آن ها بتوانند فعالیت های بدافزاری مخربی را صورت دهند و باینری بدافزار حملات دیداس و باج افزاری به دستگاه های قربانیان را رمزگشایی کنند. بورات شامل کدی است که حملات منع سرویس یا همان دیداس را راه اندازی می کند، سرعت پاسخ سرویس ها به کاربران را کاهش می دهد و موجب آفلاین شدن سایت ها می شود.

بورات همچنین می تواند ضمن انتقال پی لود باج افزار به دستگاه قربانی، فایل های کاربران را رمزنگاری و از قربانیان تقاضای باج کند. این بسته باج افزاری همچنین شامل یک فایل اجرایی کلید نگار است که ضربات کیبورد کامپیوترهای قربانیان را کنترل و آن ها را در یک فایل .txt ذخیره سازی می کند. (به منظور سرقت یا دسترسی غیر مجاز به اطلاعات کامپیوتری) **از دیگر قابلیت های بورات می توان به موارد زیر اشاره کرد:**

- **پراکسی معکوس برای محافظت از هکر**
- **قابلیت سرقت داده های احراز هویت از مرورگرها یا توکن های دیسکورد**
- **وارد کردن کد مخرب به فرآیندهای قانونی و مجاز**

بورات برای ترساندن و اذیت کردن قربانیان این فعالیت ها را انجام می دهد:

- **خاموش و روشن کردن مانیتور**
- **مخفی کردن یا نشان دادن ویژگی های دسکتاپ مانند دکمه استارت**
- **پخش کردن صوت های دلخواه**
- **خاموش و روشن کردن وبکم**
- **ضبط کردن صدا یا فیلم از وبکم و سیستم کامپیوتر**

تنها یک کلیلک تصادفی بر روی یک لینک یا فایل ضمیمه می تواند دسترسی کامل سیستم های یک سازمان را به بورات واگذار کند!

بورات یکی از جنجالی ترین فیلمهای کمدی چند دهه اخیر سینمای دنیا بود که در سال ۲۰۰۶ اکران شد. فیلمی که حواشی آن حتی تا امروز نیز ادامه داشته و منجر به اتخاذ تصمیم اساسی سیاستمداران قزاقستانی برای سرمایه گذاری در بخش فرهنگ این کشور برای به تصویر کشیدن چهره ای متفاوت از این کشور در نزد مردم جهان شده است! « بورات » با تمام حواشی اش، اما یک تجربه منحصر به فرد محسوب می شد و فیلمنامه آن به حدی چند لایه بود که بتواند نامزدی اسکار را برای خالقش، ساشا بارون کوهن به همراه داشته باشد. سری دوم نیز ساخته شد. حدوداً بیست سال پیش، این ترول حرفه‌ای نوع خاصی از کمدی را بنا نهاد که بهترین راه برای توصیف آن «دوربین مخفی روی اسید» است. هدف از دوربین مخفی، در ساده‌ترین حالتش، این است که یک آدم از همه‌جا بی‌خبر را سرکار گذاشت. اما شیوه‌ی سر کار گذاشتن کوهن آنقدر پیشرفته و دیوانه‌وار است، به چنان درجه‌ای از بداهه‌گویی و ابتکار عمل از جانب خودش نیاز دارد و گاهی آنقدر از لحاظ مالی و جانی خطرناک می شود که مقایسه کردن آن با دوربین مخفی‌های معمولی بی‌انصافی است. شاید بتوان گفت دلیل نام گذاری بدافزار مذکور به بورات، همین اذیت و آزارهای مشابه و سرکار گذاشتن مردم باشد.



گسترش وب تاریک و ارزش نظارت بر آن



امروزه بسیاری از متخصصان امنیتی، دارک وب یا وب تاریک را با برخی افشاها مانند اعتبارنامه‌های لو رفته از استفاده مجدد از رمز عبور کارمندان، مرتبط می‌دانند. این یک تهدید به حساب می‌آید؛ در ۶ سال گذشته، پلتفرم فلیر (Flare) بیش از ۱۲ میلیارد اعتبار لو رفته را مشخص کرد. دارک وب همراه با انواع جرایم سایبری به سرعت در حال رشد است. ارزش نظارت بر آن نیز همین منوال را طی می‌کند. اریک کلی (Eric Clay)، متخصص ریسک حاکمیت و انطباق، تجزیه و تحلیل داده‌ها و تحقیقات امنیتی و معاون بازاریابی در فلیر، ارائه دهنده راه‌حل نرم‌افزار به عنوان سرویس (SaaS) مدیریت مواجهه با تهدید، دراین خصوص مقاله‌ای نوشته که به شرح زیر است :

اکوسیستم جرایم سایبری اکنون نه تنها شامل پلتفرم‌های ارتباطی خصوصی مانند «I۲P» و «Tor» می‌شود، بلکه به وب‌سایت‌های شفاف و کانال‌های تلگرام نیز دسترسی دارد.

نظارت بر وب تاریک

ارزش ملموسی در نظارت بر تاریک وب برای خطرات احتمالی وجود دارد. در ادامه برخی تهدیدات احتمالی که ممکن است با آنها روبرو شوید، آورده شده است.

بدافزار اینفستیلر «Infostealer»

لاگ‌های سرقت‌کننده با دسترسی شرکتی احتمالاً یکی از مهم‌ترین عوامل برای نقض داده‌ها و حملات باج‌افزار امروزی هستند. انواع Infostealer مانند «RedLine»، راکون (Raccoon)، ویدار (Vidar)، تیتان (Titan) و آرورا (Aurora) رایانه‌ها را آلوده، سپس اثر انگشت مرورگر حاوی تمام رمزهای عبور ذخیره‌شده در مرورگر را استخراج می‌کنند. سپس عوامل تهدید نتایج را در بازارهای دارک وب یا کانال‌های تلگرام می فروشند.

این گزارش‌ها سپس برای حملات تصاحب حساب، سرقت ارزهای دیجیتال یا به عنوان دسترسی اولیه برای حملات باج افزار استفاده می‌شوند. Flare بیش از ۲۰ میلیون گزارش سرقت اطلاعات را رصد کرده و در حال اضافه کردن یک میلیون گزارش جدید در ماه است که بسیاری از آنها حاوی اعتبارنامه به چندین برنامه شرکتی هستند. ما معتقد هستیم که چیزی بین ۲ تا ۴ درصد از گزارش‌ها شامل دسترسی به محیط‌های فناوری اطلاعات شرکت‌ها هستند که در صورت به خطر افتادن می توانند خطرات قابل‌توجهی ایجاد کنند. برای شناسایی عوامل مخربی که گزارش های سرقتی را در سراسر دارک وب و تلگرام توزیع می‌کنند، شرکت‌ها می‌توانند هرگونه گزارشی را که شامل دسترسی به دامنه شرکتی داخلی است، مانند «sso.companyname.com»، نظارت کنند.

کارگزاران دسترسی اولیه

دلالان دسترسی اولیه (IAB) در تالارهای گفتگوی دارک وب مانند «XSS» و «Exploit.in» فعال هستند. این دلال‌ها دسترسی اولیه به شرکت ها را ایجاد می‌کنند و آنها را مجدداً در حراج ها و موضوعات انجمن، معمولاً با قیمت ۱۰ هزار تا ۵۰۰ هزار دلار در هر فهرست، بسته به شرکت و سطح دسترسی، می‌فروشند.

یک فهرست معمولاً شامل موارد زیر است :

- تعداد دستگاه‌ها و خدمات به خطر افتاده
- صنعت شرکت قربانی
- آنتی ویروس یا پلت‌فرم شناسایی و پاسخ نقطه پایانی که شرکت از آن استفاده می‌کند
- درآمد شرکت
- تعداد کارکنان
- موقعیت جغرافیایی شرکت
- هاست‌ها یا سرورهای در معرض خطر

عوامل تهدید می‌توانند این دسترسی را خریداری و از آن برای استقرار باج‌افزار یا سرقت داده های حساس یا منابع مالی استفاده کنند. نظارت بر انجمن‌های دلال‌های دسترسی اولیه می‌تواند هشدارهای اولیه را در مورد اینکه عوامل مخرب دستگاه‌ها را به خطر انداخته‌اند، ارائه دهد. دلال‌ها هرگز نام دقیق شرکت را لیست نمی کنند، اما به طور کلی جزئیات کافی را ارائه می دهند که اگر سازمان شما قربانی باشد، شانس معقولی وجود دارد که بتوانید آن را شناسایی کنید.

دلال‌های دسترسی اولیه همچنین عمداً به دنبال سیاهه‌های سرقت برای دسترسی به زیرساخت‌های فناوری اطلاعات هستند. یک دلال ممکن است یک دستگاه آلوده را به قیمت ۱۰ دلار از روسیه مارکت خریداری، از اعتبارنامه‌ها برای دستیابی به دسترسی، افزایش امتیازات استفاده، سپس دسترسی برای فروش را در Exploit.in با قیمت‌هایی که از ۲۰ هزار دلار شروع می‌شود، فهرست کند.

صفحات نقض اطلاعات و اخاذی باج‌افزاری

باج‌افزار آن چیزی نیست که قبلاً بود. گروه‌های باج افزاری در حال غیرمتمرکز شدن هستند و بسیاری از گروه‌ها کد منبع را برای باج‌افزار ارائه و کار آلوده کردن شرکت‌ها را برای کاهش پرداخت باج به شرکت های وابسته واگذار می‌کنند. علاوه بر این، فراگیر بودن راه‌حل‌های پشتیبان و بازیابی باعث شده که بسیاری از گروه‌ها به طور کامل رمزگذاری را کنار بگذارند و به جای آن بر تاکتیک‌های استخراج داده از جمله سرقت و افشای داده‌ها، هدف قرار دادن کارکنان یا اشخاص ثالث سازمان قربانی تمرکز کنند. یکی دیگر از روندهای نگران کننده مجرمان سایبری، اخاذی باج‌افزاری و وبلاگ‌های نقض داده است. عوامل تهدید از این وبلاگ‌ها برای اخاذی از قربانیان با تهدید به افشای اطلاعات حساس در صورت عدم پرداخت باج استفاده می‌کنند. این تاکتیک ثابت کرده که بسیار مؤثر است، زیرا سازمان‌ها از عواقب قانونی و اعتباری بالقوه‌ای که می‌تواند ناشی از نقض داده‌ها باشد، می‌ترسند. علاوه بر این، برخی گروه‌ها فایل‌ها را به صورت دسته‌ای منتشر و تایمرهای شمارش معکوس برای انتشار داده‌های حساس را اضافه می‌کنند و کارکنان فردی را برای افزایش فشار هدف قرار می‌دهند. در نتیجه، بسیاری از قربانیان تصمیم به پرداخت باج می‌گیرند؛ این امر چرخه جرایم سایبری را تداوم می‌بخشد و حملات بیشتر را تشویق می‌کند. سازمان شما احتمالاً می‌داند که قربانی باج افزار شده است یا خیر؛ با این حال، بسیاری از سازمان‌ها به دلیل نقض‌های شخص ثالث از قرار گرفتن در معرض داده‌ها رنج می‌برند. با نظارت فعالانه بر وبلاگ‌های باج‌افزاری مانند لاک بیت (LockBit)، می‌توانید قرار گرفتن در معرض داده های ناخواسته از طرف اشخاص ثالث را شناسایی و به سرعت رویه‌های واکنش به حادثه را آغاز کنید.

شناسایی تهدیدات وب تاریک

برای سازمان‌ها بسیار مهم است که بتوانند تهدیدات را در سراسر وب روشن و تاریک و کانال‌های غیرقانونی تلگرام شناسایی کنند. به دنبال راه‌حلی باشید که به راحتی در برنامه امنیتی شما ادغام شود و در یک پلتفرم اطلاعات پیشرفته‌ای از قرار گرفتن در معرض خطر بالقوه ارائه دهد. شما می‌خواهید حامل‌های پرخطری را شناسایی کنید که می‌توانند به عاملان تهدید در دسترسی به محیط شما و نظارت مستمر بر دستگاه‌های آلوده، قرار گرفتن در معرض باج‌افزار، اسرار عمومی گیت‌هاب (GitHub)، اعتبارنامه های لو رفته و موارد دیگر کمک کنند.

بررسی کتاب «هنر قانون سایبری و جرایم سایبری»

هنر و سایبر

در این عصر دیجیتال که مرزهای میان دنیای واقعی و مجازی هر روز در حال کم رنگ تر شدن است، **اهمیت و پیچیدگی قلمروی قوانین و جرایم سایبری به صورت فزاینده ای در حال افزایش می باشد.** کتاب «هنر قانون سایبری و جرم سایبری» نوشته دکتر نیوال چادهری می تواند چراغ هدایت کننده ای باشد که در این دورنمای پیچیده و نا مشخص سایبری افراد را از مسائل مختلف مربوط به این حوزه به صورت جامع آگاه می کند. نگرش دکتر چادهری از همان ابتدا نسبت به این موضوع قابل تحسین است. وی استادانه با ادغام استدلال های آکادمیک و موارد مرتبط با آن در دنیای واقعی، کتاب نام برده را به یک منبع مناسب برای متخصصین حوزه قضایی و افراد علاقه مند به این موضوع تبدیل کرده است. تحقیقات و بررسی های گسترده وی، فهم عمیقی را در مورد ابعاد چندگانه جرایم سایبری به مطالعه کنندگان این کتاب می بخشد. یکی دیگر از ویژگی های برجسته این کتاب، استفاده از نمونه های جرم سایبری بین المللی است که در دنیای واقعی اتفاق افتاده است. این مورد می تواند زندگی واقعی را به دنیای انتزاعی قوانین سایبری تزریق کند. دکتر چادهری در این کتاب معمولا قوانین نامناسب کشورهای دیگر را مورد بررسی قرار می دهد و به روشنگری مورد نحوه تاثیرگذاری این قوانین بر روی جرایم سایبری می پردازد. وی در این کتاب چارچوب های پیچیده قضایی را به زبان ساده به افراد انتقال می دهد. دکتر چادهری موضوع مهم و اساسی حق فراموش‌شدن (Right To Be Forgotten) و مباحث قانونی حول محور آن را نیز در این کتاب مطرح کرده است. حق فراموش‌شدن (RTBF) یک مفهوم حقوقی نسبتاً جدید است که پیامدهای زیادی برای سیاست‌های اینترنت، آزادی بیان و حریم خصوصی دارد. حق فراموش شدن، حق حذف اطلاعات خصوصی افراد از جست وجوهای اینترنتی و سایر دایرکتوری‌ها تحت شرایطی است.



Author
Dr. Newal Chaudhary
Advocate & Asst. Prof. of Law, T.U.

یکی دیگر از موارد مورد بحث در این کتاب، نیاز مبرم کشور نپال برای قانون گذاری مجدد در حوزه مبارزه موثر با جرایم سایبری است. علاوه بر متخصصین قضایی، قانون گذاران و شهروندان دغدغه مند در مورد بهبود سطح امنیت سایبری نیز می توانند از این کتاب بهره مند شوند و اطلاعات ارزشمندی را دریافت کنند. موارد مربوط به حریم خصوصی و قوانین شبکه های اجتماعی، قراردادهای الکترونیکی و قوانین مربوط مالیکت معنوی نیز در این کتاب پوشش داده شده اند. این ویژگی ها به مطالعه کنندگان کتاب مذکور کمک می کند تا دانش لازم در مورد حقوق و وظایف خود در قلمروی دیجیتال را به دست بیاورند. خواندن این کتاب برای کسانی که به دنبال پیمایش در دنیای پیچیده قوانین و جرایم سایبری هستند، از واجبات به شمار می آید. یکی دیگر از تمرکزات اصلی این کتاب بر روی تهاجمات سایبری برآمده از هوش مصنوعی است. دکتر چادهری تمرکز ویژه ای را بر روی چالش های نوظهور برآمده از فناوری های جدید مانند یادگیری ماشینی و هوش مصنوعی دارد. عنوان این کتاب نیز خود نیاز به توجه ویژه ای دارد. دکتر چادهری به خوبی در این عنوان توانسته اهمیت حوزه مورد بحث را به نمایش بگذارد. در این عنوان به مهارت، چیره دستی و دقت حداکثری مورد نیاز برای مجرمین سایبری و عاملین بازدارنده آن ها اشاره غیر مستقیم شده است. این بدین معناست که هر دو طرف درگیری (مجرمین سایبری و عاملین بازدارنده آن ها) بایستی هنر و مهارت کافی را در این حوزه کسب کنند تا بتوانند از یکدیگر پیشی بگیرند. هنر قوانین سایبری و جرایم سایبری چیزی بیش از یک کتاب ساده است و مانند یک فانوس می تواند ما را به سوی یک دنیای دیجیتال ایمن هدایت کند.

سینما سایبر



مقدمه

با توجه به نو ظهور بودن اصطلاح سایبر سینما کاملا روشن است که رسیدن به تعریفی واحد و بی‌تردید از این مفهوم چندان کار آسانی نخواهد بود.به همین دلیل در این قسمت سعی بر این خواهد بود که حداقل چند تعریفی که نگارنده به آنها برخورد کرده است، بیان شود.

همانطور که می‌دانیم فضای سایبر از امکان تعاملی بودن بر خوردار است، تعاملی که حتی در امور تبلیغاتی و جذب اگهی بسیار به کمک سینما آمده است. همانطور که در ابتدا گفته شد سینما پدیده ای نیازمند معرفی و تبلیغ است تبلیغی که امکانش در فضای سایبر با شرایط مربوط به خودش فراهم شده است به طوری‌که در حال حاضر این امکان فراهم آمده که همگام با امکانات دیگر این فضا در کنار سینما به اقتصاد آن یاری رساند.

در فضای سایبر امکان پخش با قدرت انتخاب هم زمان خواهد بود به این ترتیب که به دلیل تعاملی بودن این فضا این امکان در اختیار مخاطب قرار گرفته که خود روند داستان فیلم را تحت تاثیر قرار دهد و در واقع داستان را همانگونه که می‌خواهد پیش ببرد و پایان دلخواه خود را برای آن رقم بزند.

فضای سایبر با از بین بردن محدودیت‌های زمانی و مکانی ارتباط تولیدکنندگان در تولید فیلم را فراهم کرده است به نوعی که چند نفر در جای جای دنیا می‌توانند همزمان با یکدیگر به تولید یک فیلم بپردازند و هر کسی در ساخت آن مسئولیتی را بر عهده گیرد. علاوه بر این سینمای سایبر امکان تماشای همزمان فیلم را نیز فراهم کرده است به طوریکه دیگر لازم نیست مخاطبان برای تماشای فیلم در یک مکان تعریف شده‌ای به نام سینما حضور یابند بلکه آنها می‌توانند فیلم دلخواه خود را در این فضا انتخاب کرده و با بازکردن آن در مکان دلخواه خود به تماشایش بپردازند و البته این تماشای مستقل تعارضی با همزمانی تماشا با دیگرمخاطبان ایجاد نخواهد کرد به طوریکه ممکن است مخاطبی دیگر در مکان جغرافیایی متفاوتی در همان زمان مشغول تماشای فیلم باشد. اما فارغ از این‌ها تعریفی دیگر از سایبر سینما ارائه شده که بیش از تعاریف دیگر مورد علاقه نگارنده است و آن به شیوه بازنمایی انقلاب دیجیتال در سینما مربوط می‌شود.

آینده فیلم های سینمایی

هوش مصنوعی این روزها نقش کلیدی و مهمی در جامعه بشری ایفا می کند. امروزه به هر گوشه و کناری که نگاه می کنیم، ردی هم از تکنولوژی و هوش مصنوعی می‌بینیم. این تکنولوژی جذاب و پر سر و صدا در همه صنایع از صنعت خودروسازی و ماشین سازی گرفته تا بازی‌های ویدیویی و فیلم های سینمایی از آن استفاده می شود. همین دلیل باعث شده است که بسیاری از دانشمندان آینده بشر را در دستان هوش مصنوعی ببینند. احتمالات مختلفی برای آینده بشر با حضور هوش مصنوعی در نظر گرفته شده است و همچنین بیش از ۱۰۰ اثر سینمایی در مورد هوش مصنوعی و اثرات آن بر زندگی انسان‌ها ساخته شده است که همین مسئله آن را به یک موضوع مورد بحث بدل کرده است.

آیا هوش مصنوعی در مجموع برای صنعت فیلم خوب است؟

هوش مصنوعی روی هم رفته نگرانی‌های بسیاری در عموم مردم برانگیخته است؛ به طور واضح و مهم‌تر از همه، مردم از این موضوع ترس دارند که دیگر نیاز به شغل‌هایی که قبلاً توسط انسان ها انجام می‌شد نباشد و به زبان ساده، کارشان را از دست بدهند. به عنوان مثال، افرادی که در غرفه فروش بلیت کار می‌کنند با کاربردی شدن برخی از برنامه‌هایی که در بالا از آن‌ها نام برده شد، ممکن است از کار اخراج شوند. با این حال، استفاده از هوش مصنوعی ممکن است تنها شانس صنعت فیلم سازی برای تطبیق دادن خود با دنیای دیجیتال امروز و زنده ماندن در آینده باشد. علاوه بر این، به عنوان اتفاقی بسیار جالب و شگفت انگیز، در حال حاضر به نظر می‌رسد که هوش مصنوعی در واقع بیش از آنکه شغل از بین ببرد، شغل ایجاد می‌کند! به این معنی که کارکنان و کارفرمایان باید بتوانند مجموعه مهارت‌های خود را با شیوه‌های جدید خدمات‌دهی انطباق دهند. طبیعتاً برخی هنوز نمی‌دانند چگونه باید این کار را انجام دهند. از این زاویه، هوش مصنوعی برای صنعت فیلم خوب است. همان‌طور که شرکت فست گزارش می‌دهد، تکنولوژی هوش مصنوعی به معنای واقعی کلمه به بهبود طرح‌های داستانی مورد استفاده در فیلم ها و همچنین نظارت بر فیلم‌هایی که احساسات مناسب و جذابی در مخاطبان ایجاد می‌کنند، کمک کرده است. با استفاده از اطلاعات و داده‌های هوش مصنوعی برای نظارت بر واکنش‌های بینندگان، ارائهٔ فیلم‌ها به مصرف‌کنندگان بهبود پیدا کرده است. در واقع، به‌طورکلی سینما و بازیگری با استفاده از هوش مصنوعی به‌سوی آینده حرکت می‌کنند. همان‌طور که می‌دانیم، هوش مصنوعی در تجربیاتی که در سنت‌های قدیمی بازیگری و نمایش جریان دارد نیز حضور دارد؛ "هنرهای نمایشیِ تعاملی" که در آن مخاطب با استفاده از تکنولوژی عینک های واقعیت مجازی، خود در میانهٔ صحنهٔ نمایش حضور دارد، تجربه‌ای محبوب به وجود آورده و ثبت کرده‌اند. هرچند که هنوز فراگیر نشده است .



نگاهی به فیلم سینمایی ناشنیده(The Unheard)

فرافرکانس!

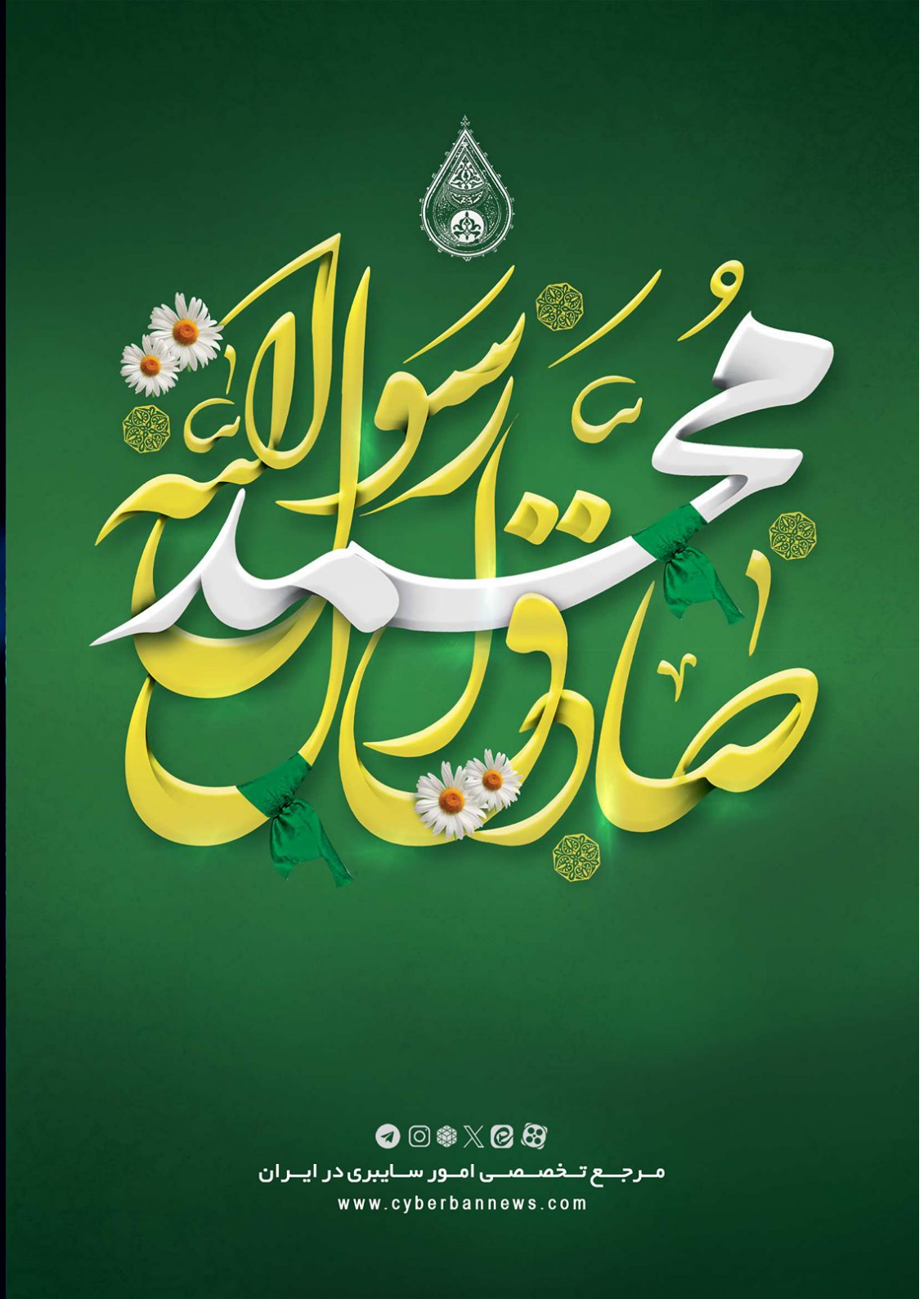
هوشمندسازی انسان همواره یکی از زمینه‌های پژوهشی پرطرفداری بوده که به موازات پیشرفت هوش مصنوعی مورد تاکید قرار گرفته است. دستیابی به توانایی‌هایی که انسان را به اَبَرانسان تبدیل می‌کند. روزی را متصور باشید که با یک دوز تزریق از یک فرمول خاص توانایی بویایی یا بینایی شما چند برابر شود. مثلا چشم شما تبدیل به یک دوربین حرارتی شود؛ مردمک چشمانتان توانایی تمیز فرکانس‌های مختلف نوری را داشته باشد! قطعا این انسان در جنگ احتمالی با هوش مصنوعی گستاخ، از شانس حیات بیشتری برخوردار است.. جفری براون در «ناشنیده» اگرچه مستقیما به سراغ یک ماجرای سایبری نرفته و روایت را بیشتر به سمت سینمای وحشت برده است اما، توجیه علمی آنچه بر کاراکتر کلویی گذشته را به خوبی به تصویر کشیده. در سکانسی که کلویی به اتاق کار جاشوا می رود، با تعدادی اسپیکر و دتکتور صوتی مواجه می شویم. صداهای نویز مانند و آزاردهنده‌ای نیز محیط را احاطه کرده است. جاشوا می‌گوید این فراصوت است؛ اصواتی که در بازه شنوایی انسان قرار ندارند و در مرز آستانه شنوایی نیز به صورت نویزهای آزاردهنده شنیده می‌شوند. اما سیستم شنوایی کلویی قادر به آشکارسازی این فراصوت است. او مکالماتی که در کودکی با مادرش داشته و اکنون بصورت فراصوت در محیط موجود است را می‌شنود. صداهایی که در گوشه و کنار خانه به دام افتاده است؛ طول موجشان تغییر کرده اما نابود نشده‌اند. درواقع تزریق یک ژن مولد با همراهی یک ویروس نفوذگر، آستانه شنوایی او را افزایش داده است!.

داستان فیلم

کلویی گریدن، دختر ۲۰ساله‌ای است که در کودکی و پس از ابتلا به مننژیت، قدرت شنوایی خود را از دست داده است. او به عنوان نمونه پژوهشی برای پیشبرد روش درمانی جدیدی انتخاب می‌شود. در این تکنیک جدید، ژنی که مسئول رشد سلولی مربوط به اندام شنوایی است، توسط یک ویروس پسگرد به داخل گوش تزریق می‌شود. با انتقال ژن به محل مورد نظر، تارهای عصبی آسیب دیده مجددا شروع به رشد می‌کنند و حس شنوایی رفته رفته ترمیم می شود.کلویی پس از انجام مرحله نخست درمان و برای گذر از دوران نقاهت به خانه جنگلی دوران کودکی‌اش نقل مکان می‌کند. سال ها قبل مادر کلویی در همین منطقه مفقود شده است. قرار است پدر کلویی طی چند روز آینده برای فروش این خانه به او ملحق شود. پس از گذشت چند روز از اقامت کلویی در خانه قدیمی، حس شنوایی او برمی‌گردد. شنیدن اصواتی که او سال‌ها از درکشان محروم بوده برای او شیرین است. ذهن کلویی همچنان درگیر سرنوشت مادرش است. اکثر اوقات او به تماشای فیلم‌های خانوادگی باقی مانده از دوران کودکی می‌گذرد. مورد عجیب اما، صداهای نامفهومی است که از گوشه و اطراف خانه به گوش کلویی می‌رسد؛ اصواتی گنگ و نامفهوم. جاشوا، هم‌بازی دوران کودکی کلویی که به مسائل فیزیکی علاقه‌مند است، متوجه وجود نوع عجیبی از امواج فراصوت در منطقه شده است؛ امواجی که البته توسط حس شنوایی کلویی قابل آشکارسازی است و ... .

فیلم سینمایی «ناشنیده– The Unheard» هم اکنون از طریق پلتفرم‌های داخلی نمایش آنلاین، در دسترس علاقه‌مندان قرار دارد.


بنیاد
شهید
و امور ایثارگران
جمهوری اسلامی ایران
وزارت امور خارجه
هفت هشتاد
حملات سایبری اخیر علیه جمهوری اسلامی ایران
در حملات سایبری اخیر، شاهد بودیم که سایت وزارت امورخارجه، بنیادشهید، نرم افزار ۷۸۰، تپسی و سایت سازمان ثبت احوال مورد هدف هکرها قرار گرفت؛ به راستی که حفاظت از داده های شهروندان و تأمین امنیت سایبری به عهده کدام نهاد است؟


مرجع تخصصی امور سایبری در ایران
www.cyberbannews.com