دریچه فناوری

بیابیز ۱۴۰۳

فناوری دریچه

نشریه شماره ۱

در این شماره می خوانیم:

- بررسی کاربردهای هوش مصنوعی در استراتژی های دفاعی اسرائیل
- مقدمه ای بر فناوری های فایروال
- سازمان امنیت ملی آمریکا
- جرایم رایانه ای

بسمه تعالی

فهرست

سازمان حراست کل کشور
حراست کل استان البرز

فناوری دریچه

مدیر مسئول:
محمد شجاعی
سردبیر:
مریم دهقانی
اعضای هیئت تحریریه:
محمد شجاعی
الهام همتی
حمیدرضا کاوسی
مریم دهقانی
طراحی و صفحه آرایی:
سید مهدی حسینی

KHAMENEI.IR
دفتر حفظ و نشر آثار حضرت آیت الله العظمی خامنه‌ای

تأکیدات مهم مقام معظم رهبری(مدظله العالی) در خصوص مدیریت فضای مجازی (قسمت دوم):

نباید فضای مجازی را در اختیار دشمن گذاشت.

حضرت آیت الله خامنه ای تاکید کردند: «همه دنیا و همه کشورهای دنیا روی فضای مجازی خودشان دارند اعمال مدیریت می‌کنند. اما ما افتخار می‌کنیم به اینکه فضای مجازی را ول کردیم. این افتخار ندارد. این به هیچ وجه افتخار ندارد؛ فضای مجازی را باید مدیریت کرد. باید از این امکان، مردم استفاده کنند. فضای مجازی بلاشک برای مردم وسیله آزادی است و خیلی هم خوب است. اما نباید این وسیله را در اختیار دشمن گذاشت که بتواند علیه کشور و ملت توطئه کند. دشمنان دارند از این فضا استفاده می‌کنند. رهبر انقلاب در سال ۹۹ نیز فرمایشات داهیانه با تاکید بر رویکرد فرصت محور در مواجهه با فضای مجازی داشته‌اند که چراغ‌های آگاهی بخش در انتخاب مسیر حکمرانی فضای مجازی را روشن می‌کند.

قوت در فضای مجازی حیاتی است.

مقام معظم رهبری در ابتدای سال ۹۹ و در سخنرانی نوروزی نیز خطاب به ملت ایران فرمودند: «امروز قوت در فضای مجازی حیاتی است؛ امروز فضای مجازی حاکم بر زندگی انسان‌ها است در همه دنیا؛ و یک عده‌ای همه کارهایشان را از طریق فضای مجازی پیش می‌برند؛ قوت در این زمینه حیاتی است. یا مثلاً قوت در زمینه بهداشت و درمان حیاتی است؛ که بحمدالله در این زمینه محققان و پزشکانمان و کسانی که در این راه خبره هستند کار زیادی انجام داده‌اند.

سخن سردبیر

جنگ الکترونیک در دنیای مدرن

دنیای امروز با چالش‌های جدی در عرصه جنگ و صلح روبرو است و یکی از ابعاد جدید و حیاتی این چالش ها، جنگ الکترونیک است. با پیشرفت سریع فناوری‌های دیجیتال، جنگ‌ها به دنیای سایبری گسترش یافته و به جای میدان‌های نبرد سنتی، در بسترهای مجازی و الکترونیکی صورت می‌گیرند. جنگ الکترونیک یا (EW Electronic Warfare) یک جزء حیاتی است که نیروهای مسلح را قادر می‌سازد تا ارتباطات و سیستم‌های تسلیحاتی دشمن را مختل یا دستکاری کنند، از این رو به بخشی جدایی‌ناپذیر از سیاست‌ها و استراتژی‌های ملی همه کشورها تبدیل شده است. از این جنگ ها به عنوان جنگ‌های نامرئی و پیچیده نیز یاد می شود؛ تأثیرات آن‌ها بر زندگی روزمره غیرقابل انکار است، از تهدید به زیرساخت‌های حیاتی گرفته تا تأثیر بر افکار عمومی. این نوع جنگ، ابعاد جدیدی از استراتژی نظامی را می‌طلبد که در آن ماهیت‌های سنتی جنگ، از جمله قدرت و قدرت نمایی، با مفاهیم نوین فناوری و اطلاعات ترکیب می‌شوند.

متداول ترین انواع جنگ الکترونیک عبارتند از پارازیت که در دسته اقدامات متقابل الکترونیکی (ECM) قرار می گیرد و رهگیری سیگنال (SIGINT). هدف از پاسخ راهبردی به ECM، محدود کردن توانایی دشمن برای تبادل اطلاعات از طریق نادیده گرفتن انتقال رادیویی، ارسال سیگنال برای جلوگیری از شناسایی رادار و انتقال اطلاعات نادرست است. جمع آوری اطلاعات با افزایش پیچیدگی فنی جنگ های مدرن اهمیت بیشتری یافته است و اکنون نقش مهمی در تعیین اینکه آیا دولت ها در وهله اول وارد جنگ می شوند یا خیر، ایفا می کند. در ماه نوامبر، اوکراین با تاکتیک‌های پیچیده جنگ الکترونیکی روسیه مواجه شد که شامل اختلال در سیستم های ارتباطی و راداری می‌شد که به شدت بر اثربخشی نظامی اوکراین تأثیر گذاشت. نیروهای روسی از EW برای ایجاد سردرگمی و برهم زدن هماهنگی نیروها استفاده کردند و نقش تعیین کننده EW را در جنگ مدرن به نمایش گذاشتند. از این رو کشورها به دنبال بهبود قابلیت‌های خود در دفاع از زیرساخت‌های حیاتی و محافظت از اطلاعات حساس می‌باشند و این موضوع در کل روندهای سیاسی، اقتصادی و اجتماعی تأثیرگذار است. در مجموع می توان گفت که آگاهی نسبت به این پدیده و بررسی ابعاد آن، از اهمیت ویژه‌ای برخوردار است.

در پایان بر خود وظیفه می دانم از تلاش بی‌وقفه و متعهدانه همکاران بزرگواری که در تهیه و انتشار شماره پنجم نشریه دریچه فناوری ما را همراهی کردند، تقدیر و تشکر نمایم. همچنین حمایت‌ها، نظرات و پیشنهادات شما خوانندگان عزیز بی شک ما را در مسیر بهبود و پیشرفت یاری می‌رساند. امید است همچنان با همراهی و محبت شما، بتوانیم گام‌های بزرگ‌تری در حوزه علم و فناوری برداریم.

ضمنا به منظور دسترسی آسان به نسخه الکترونیکی نشریه دریچه فناوری، این نشریه در سایت حراست کل استان البرز بارگذاری شده است.

با تقدیم احترام
مریم دهقانی

صراط

قسمت پنجم

در برخی موارد پیامبر اکرم (ص) به ماموران جمع آوری اخبار و اطلاعات امر می‌کردند اخبار و اطلاعات جمع آوری شده را تنها در اختیار حضرت بگذارند و از دیگران پوشیده دارند. برای مثال در جنگ احد جباب بن منذر را برای کسب خبر از دشمن اعزام کردند و به او فرمودند: «چون برگشتی، در حضور هیچ یک از مسلمانان به من گزارش مده، مگر زمانی که تعداد آن ها بسیار اندک باشد.»
در جنگ بنی قریظه نیز چند نفر را فرستادند و به آن ها فرمودند:
بروید و تحقیق کنید که آیا آنچه از بنی قریظه مبنی بر پیمان شکنی و همدستی با قریش و احزاب در جنگ خندق خبر یافته‌ام، راست است یا دروغ؟ اگر راست بود سخن با اشاره و کنایه بگویید که من بفهمم و مردم را سست نکنید و اگر به پیمان خود وفادار باشند آشکارا و در حضور مردم بگویید.
هرچند این دو نقل تاریخی درباره حفاظت از اخبار جمع آوری شده از دشمن است، می‌توان استنباط کرد اگر اسرار مربوط به دشمن را در شرایطی نباید افشا کرد اسرار مربوط به نیروهای خودی را به طریق اولی نباید افشا کرد؛ همچنان که زمان جنگ و اسرار نظامی خصوصیت و ویژگی خاصی نداشته، بلکه حفاظت از آنچه در نظام اسلامی جزء اسرار شمرده می‌شود، نیز واجب است.
تاکتیک تقیه نیز که در بخش احادیث به عنوان تاکتیکی جهت حفاظت از اسرار و اشخاص بیان شد، در سیره عملی امامان معصوم(ع) دیده می شود. از جمله داوود بن حصین با واسطه نقل می کند:

امام صادق علیه السلام درباره روزهایی که در زمان ابوالعباس سفاح در حیره بودند، چنین فرمودند:
من پیش ابوالعباس رفتم. مردم از اینکه آن روز ماه رمضان است یا نه در شک بودند، با اینکه به خدا سوگند ماه رمضان بود. سلام کردم. پرسید: ای اباعبدالله شما روزه دارید؟ گفتم: نه. سفره غذا مقابل ابوالعباس بود. گفت: بفرمایید بخورید. من جلو رفتم، خوردم و گفتم روزه را به دستور تو می‌گیرم و به دستور تو می‌خورم.
آن مرد (راوی حدیث) به امام صادق(ع) گفت: در ماه رمضان روزه خوردید؟ حضرت پاسخ دادند: «آری. به خدا قسم، یک روز از ماه رمضان را روزه بخورم، بهتر است از اینکه گردنم زده شود.»
نامشخص بودن راوی با توجه به محتوای اطلاعاتی بودن روایت، شایسته توجه است.
همچنین عبدالله بن فضل از پدر خود نقل می کند: من دربان هارون الرشید بودم. روزی او باخشم وارد شد. شمشیر در دست داشت و آن را می چرخاند. به من گفت: ای فضل، سوگند به خویشاوندی که با پیغمبر(ص) دارم، اگر پسر عمویم را نیاوری، سر از پیکرت برمی دارم. خدمت امام رسیدم، به حضرت سلام کردم و گفتم: هارون الرشید شما را خواسته است. فرمودند:
مرا با هارون چه کار؟! آیا با وجود زرق و برق و نعمت دنیا که در اختیار دارد، مرا از یاد او نبرده است؟ سپس با عجله از جای حرکت کردند، در حالی که می فرمودند: اگر در خبری از رسول الله صلی الله علیه وسلم نشنیده بودم که اطاعت از سلطان از روی تقیه واجب است، هرگز نمی آمدم.

مقدمه‌ای بر فناوری های فایروال

قسمت دوم

فایروال‌ها دستگاه‌ها یا برنامه‌هایی هستند که جریان ترافیک شبکه بین شبکه‌ها یا سرورهایی که سطوح امنیتی متفاوتی دارند، کنترل می‌کنند. اگرچه فایروال‌ها اغلب در زمینه اتصال به اینترنت مورد استفاده قرار می‌گیرند، ممکن است در سایر محیط های شبکه نیز کاربرد داشته باشند. به عنوان مثال، بسیاری از شبکه‌های سازمانی از فایروال‌ها برای محدود کردن ارتباطات شبکه‌های داخلی که برای وظایف حساس‌تر مانند امور مالی یا پرسنلی استفاده می‌شوند، بهره می‌برند. یک سازمان با استفاده از فایروال‌ها برای کنترل اتصال به این مناطق، می‌تواند از دسترسی غیرمجاز به سیستم‌ها و منابع خود جلوگیری کند. وجود یک فایروال مناسب، یک لایه اضافی از امنیت فراهم می‌کند.

چندین نوع از فناوری‌های فایروال موجود است. یکی از راه‌های مقایسه قابلیت‌های آن‌ها، بررسی لایه‌های (TCP/IP) است که هرکدام قادر به بررسی آن هستند. TCP/IP از چهار لایه تشکیل شده است که با هم کار می‌کنند تا داده‌ها را بین سیستم ها منتقل کنند. زمانی که یک کاربر می‌خواهد داده‌ها را از طریق شبکه‌ها انتقال دهد، داده‌ها از بالاترین لایه به لایه‌های واسط و سپس به پایین‌ترین لایه منتقل می‌شود، به طوری که هر لایه اطلاعات بیشتری اضافه می‌کند. پایین‌ترین لایه داده‌های جمع شده را از طریق شبکه فیزیکی ارسال می‌کند و داده‌ها سپس به وسیله اطلاعات موجود در لایه‌ها به مقصد خود منتقل می شوند. به بیانی دیگر، داده‌های تولید شده توسط یک لایه در یک ظرف بزرگتر توسط لایه زیرین محصور می‌شوند.

در لایه پیوند داده، آدرس‌هایی که به رسانه شبکه اختصاص داده می‌شوند، به آدرس مک (MAC) نامیده می‌شوند. یک مثال از این آدرس، آدرس کارت شبکه است که به صورت اختصاصی به آن تعلق دارد. سیاست‌های فایروال به ندرت به لایه پیوند داده اهمیت می‌دهند. آدرس‌ها در لایه شبکه به عنوان آدرس‌های IP شناخته می‌شوند. لایه انتقال برنامه‌های شبکه خاص و جلسات ارتباطی را به جای آدرس‌های شبکه شناسایی می‌کند؛ یک میزبان می‌تواند تعداد زیادی جلسه لایه انتقال با دیگر میزبان‌ها در همان شبکه داشته باشد. لایه انتقال همچنین می تواند شامل مفهوم پورت‌ها باشد. یک شماره پورت مقصد (destination) می تواند نشان دهنده یک سرویس باشد که در سرور مقصد روی پورت مقصد فعال باشد. پروتکل‌های انتقال مانند TCP و UDP دارای پورت هستند، در حالی که سایر پروتکل‌های انتقال دارای پورت نمی‌باشند.

ترکیب آدرس IP منبع و پورت با آدرس IP مقصد و پورت به تعریف جلسه (session) کمک می‌کند.

بالاترین لایه، برنامه‌های کاربردی می‌باشد. فایروال می‌تواند ترافیک برنامه‌ها را بررسی کرده و از آن به عنوان مبنایی برای اعمال سیاست ها استفاده کند. فایروال های ابتدایی بر روی یک یا چند لایه معمولاً لایه‌های پایین‌تر عمل می‌کنند، در حالی که فایروال های پیشرفته‌تر همه لایه‌های TCP را بررسی می‌کنند. آن‌هایی که لایه‌های بیشتری را بررسی می‌کنند می توانند آنالیزهای دقیق‌تر و جامع‌تری انجام دهند. فایروال هایی که قدرت تجزیه و تحلیل در لایه برنامه را دارند؛ می توانند برنامه‌ها و پروتکل‌های پیشرفته را بهتر مدیریت کنند و خدماتی را ارائه دهند که به کاربران اختصاص دارد. به عنوان مثال، فایروالی که فقط لایه‌های پایین را کنترل می‌کند معمولاً نمی‌تواند کاربران خاص را شناسایی کند، اما سیستمی با قابلیت‌های لایه برنامه می‌تواند تأیید هویت کاربر را اعمال کرده و مخاطرات مربوط به کاربران خاص را ثبت کند.

تکنولوژی فایروال‌ها معمولاً با دیگر فناوری‌ها ترکیب می‌شوند (به ویژه مسیریابی) و بسیاری از قابلیت هایی که غالباً با فایروال‌ها مرتبط هستند، بیشتر مربوط به این فناوری‌های ترکیب شده هستند. برای مثال، ترجمه آدرس شبکه (NAT) گاهی به عنوان یک فناوری فایروال در نظر گرفته می‌شود، اما در واقع یک فناوری مسیریابی است. بسیاری از فایروال‌ها همچنین دارای ویژگی‌های فیلترینگ محتوا برای اجرای سیاست‌های سازمانی هستند که به‌طور مستقیم مربوط به امنیت نیستند. برخی از فایروال‌ها شامل فناوری‌های سیستم جلوگیری از نفوذ (IPS) هستند، که می‌توانند به حملاتی که تشخیص می‌دهند واکنش نشان دهند تا از آسیب به سیستم های محافظت‌شده جلوگیری کنند. فایروال‌ها معمولاً در محیط شبکه قرار دارند. چنین فایروالی می‌تواند یک رابط (inter-face) خارجی و یک رابط داخلی داشته باشد، با این که رابط خارجی همان رابط بیرونی شبکه است. این دو رابط گاهی اوقات به ترتیب به عنوان محافظت‌نشده (untrust) و محافظت شده (trust) شناخته می‌شوند.

اگرچه، بیان اینکه چیزی محافظت‌شده است یا نه، نادرست است زیرا سیاست‌های فایروال می‌تواند در هر دو جهت عمل کند؛ برای مثال، ممکن است سیاستی برای جلوگیری از ارسال کد اجرایی از داخل محیط حفاظت نشده به محیط حفاظت نشده وجود داشته باشد. در شماره بعدی به جزئیات تکنولوژی های فایروال پرداخته خواهد شد.

نویسنده: محمد شجاعی

سازمان امنیت ملی آمریکا
NSA

سازمان امنیت ملی یکی از سازمان‌های دولتی آمریکا است که زیر نظر وزارت دفاع آمریکا اداره می‌شود و در سال ۱۹۵۲ به دستور رئیس جمهور وقت آن زمان، هری ترومن، تاسیس شد. این سازمان به عنوان جانشین سازمان خدمات امنیتی که در جنگ جهانی دوم فعالیت می کرد، شکل گرفت. هدف از تاسیس این سازمان، ایجاد یک سازمان مسئول جمع آوری و تحلیل اطلاعات الکترونیکی و ارتباطاتی بود. وظیفه رسمی سازمان، نظارت بر فعالیت‌های مخابراتی، ارتباطاتی و ماهواره ای و کشف رمز در آمریکا است.

وظایف NSA شامل جمع آوری، تحلیل و محافظت از اطلاعات الکترونیکی و ارتباطاتی در زمینه های سیاسی، اقتصادی، اجتماعی، فرهنگی، نظامی و علمی است. منابع NSA شامل سیستم ها، شبکه ها، دستگاه ها و افرادی است که اطلاعات الکترونیکی و ارتباطاتی را ارسال، دریافت، ذخیره یا پردازش می کنند. روش های عملیاتی NSA شامل جاسوسی الکترونیکی، جاسوسی ارتباطاتی، رمزگشایی، رمزنگاری، و امنیت سایبری است.

NSA یا سازمان امنیت ملی، یکی از قدرتمندترین و پیشرفته ترین سازمان های اطلاعاتی جهان است که وظیفه جمع آوری، تحلیل و محافظت از اطلاعات الکترونیکی و ارتباطاتی را دارد. آژانس امنیت ملی با تخصص شنود الکترونیک، مسئول نظارت جهانی، گردآوری و پردازش اطلاعات و داده، با هدف اطلاعات داخلی و خارجی و ضدتروریسم است. همچنین کار آژانس امنیت ملی، حفاظت از شبکه‌های ارتباطی و سامانه‌های اطلاعاتی ایالات متحده آمریکا است.

همچنین این سازمان وظیفه حفاظت از مکالمات دولتی و سیستم‌های اطلاعاتی آمریکا را در مقابل سازمان‌های مشابه بر عهده دارد. این سازمان یکی از محرمانه‌ترین و بزرگ ترین سازمان‌های جاسوسی به شمار می‌رود که البته فعالیت‌های آن شامل جاسوسی انسانی نیست و محدود به حوزه ارتباطات می شود.

برنامه جاسوسی جهانی "اشلون":

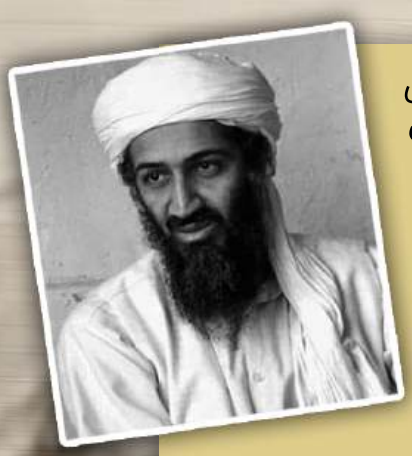
اشلون واژه‌ای است که معمولا برای اشاره به یک سیستم جاسوسی جهانی (تأسیس در سال ۱۹۴۷) که سازمان‌های اطلاعاتی پنج کشور آمریکا، انگلستان، کانادا، استرالیا و نیوزیلند در آن نقش دارند و هم‌اکنون توسط آژانس امنیت ملی آمریکا هدایت می‌شود، به کار می‌رود. اشلون مقادیر عظیم تماس‌های تلفنی، پیام‌های ایمیل، دانلودهای اینترنتی، ارتباطات ماهواره‌ای و غیره را جمع‌آوری کرده، سپس اطلاعات **مورد نظر را از طریق برنامه‌های اطلاعاتی تصفیه می‌کند.**

بنا بر گزارش ها اشلون، حدود ۹۰ درصد از ترافیک اینترنتی را وارسی می‌کند. آمریکا تلاش بسیاری کرده است تا این برنامه را از نظرها مخفی نگه دارد. اشلون یک عملیات بسیار محرمانه است که دادگاه‌ها و مجالس ملی هیچ گونه نظارتی بر آن ندارند و در نتیجه کسی نمی‌داند که این برنامه‌ها چگونه مورد استفاده قرار می‌گیرند و یا اینکه استفاده از آنها مطابق با موازین قانونی است یا نه؟

بنا به گزارشات، دولت آمریکا از برنامه اشلون برای جاسوسی صنعتی نیز بهره می‌گیرد که شامل تکنولوژی توربین بادی بدون دنده، ساخته شرکت آلمانی "انرکون" (Ener-con) و نیز تکنولوژی گفتار که ساخته شرکت بلژیکی "هاسپی‌اند لرناوت" (Lernout&Hauspie) می باشد. جاسوسی‌های اقتصادی حتی به داخل آمریکا نیز سرایت کرده است. بر این اساس، برخی شرکت‌های آمریکایی مجبور می‌شوند تا از **معاملات به نفع شرکت‌هایی که به طور مداوم پول به سوی دو** حزب حاکم در آمریکا سرازیر می‌کنند، کنار بکشند.

آژانس امنیت ملی و حملات یازده سپتامبر:

نقش آژانس امنیت ملی آمریکا در حملات یازده سپتامبر چیست؟ این سؤالی است که هیچگاه به صورت مشروح مورد بررسی قرار نگرفت.



با این وجود، شاید این سازمان بیش از دو دستگاه امنیتی و اطلاعاتی فوق در این قضایا دست داشت زیرا حداقل از سال ۱۹۹۹ در حال استراق سمع مکالمات بن لادن با مأمورینش بود. این در حالی است که آژانس هیچ گزارشی در مورد این مکالمات به دیگر سازمان‌های اطلاعاتی ارائه نکرده و حتی نام افراد بن لادن را نیز فاش نساخت. این در حالی است که ریاست این سازمان بعدها غیرقانونی بودن شنود مکالمات در داخل آمریکا را مانعی برای مبارزه با تروریست‌ها و جمع‌آوری اطلاعات معرفی نموده و درخواست داد تا سازمان اختیارات لازم برای استراق سمع خود شهروندان آمریکا را نیز داشته باشد.

برنامه‌های NSA:

اشلون: NSA در مشارکت با آژانس‌های مشابه در انگلستان، کانادا، استرالیا و زلاندنو که با عنوان گروه UKUSA شناخته می‌شوند، بصورت گسترده‌ای بر روی سیستم‌هایی به نام ECHE-LON کار می‌کنند که انتظار می‌رود توانایی مانیتور کردن بخش عظیمی از ارتباطات تلفنی، فکسی و داده‌ای جهان را داشته باشد.

طبق یادداشتی در روزنامه New York Times به صورت فنی، تقریباً تمامی تلفن های مدرن، اینترنت، فکس و ارتباطات ماهواره‌ای به خاطر پیشرفت‌های اخیر در تکنولوژی و ماهیت فضای باز (Open Air) اغلب ارتباطات رادیویی در سراسر دنیا، قابل استخراج می‌باشند.

عملیات جمع آوری فرضی NSA بحران‌های زیادی را ایجاد کرده‌اند که اغلب به خاطر این تصور است که NSA حریم خصوصی آمریکایی‌ها را نقض می‌کند.

فعالیت درون مرزی:

برای جمع‌آوری اطلاعات فعالیت های جاسوسی خارجی در داخل مرزهای ایالات متحده به FBI وابسته است و فعالیت‌های داخلی خود را فقط به سفارت خانه‌ها و ماموریت‌های ملل بیگانه محدود کرده است.

فعالیت‌های نظارتی NSA محدود به قانون حفظ حریم شخصی آمریکایی‌ها می‌باشد، اما این محدودیت‌ها برای اشخاص غیر آمریکایی که در خارج از مرزهای آمریکا هستند، اعمال نمی‌شود. این فعالیت‌ها، بخصوص شنود تلفنی درون مرزی و برنامه های پایگاه داده تماس‌ها، سوالاتی در مورد گسترش فعالیت‌های NSA و نگرانی‌ها درمورد تهدید برای حریم خصوصی ایجاد کرده‌است.

برنامه‌های شنود سیمی (Wire-tapping):

۱. شنود سیمی درون مرزی: در دوران ریاست جمهوری ریچارد نیکسون آغاز شد و در سال های پس از کناره گیری ریچارد نیکسون، بازرسی‌هایی در مورد استفاده نادرست از امکانات CIA و NSA انجام گرفت.

۲. شنود سیمی و استخراج داده‌ها: یکی از برنامه‌های شنود سیمی بنام Thin Thread در اواخر دهه ۱۹۹۰ مورد آزمایش قرار گرفت، اما هیچ وقت مورد بهره برداری قرار نگرفت.

۳. شنود سیمی بدون پیش اجازه در دوره ریاست جمهوری جورج بوش: در دسامبر ۲۰۰۵ روزنامه نیویورک تایمز، گزارش کرد که تحت فشار کاخ سفید و دستور مستقیم رئیس جمهور بوش، سازمان امنیت ملی، در اقدامی جهت جلوگیری از اقدامات خرابکارانه، کلیه تلفن‌های اشخاص آمریکایی که با افرادی خارج از کشور تماس گرفته بودند شنود کرده است.

NSA در سال های اخیر نیروی فوق العاده ای را بر روی رمزگشایی، شکستن کد ها و عبور از سیستم های رمزنگاری پیچیده صرف کرده است.

نقشه این مرکز ۲ میلیارد دلاری که ۹۳,۰۰۰ متر مربع مساحت دارد، به این شرح است:

۱.ماهواره های ثابت: چهار ماهواره ای که در پیرامون زمین هستند، فرکانس های مختلف بی سیم را رصد می کنند. از واکی تاکی ها و تلفن های همراه در لیبی گرفته تا سیستم های رادار کره شمالی. نرم افزار این شبکه، به عنوان اولین فیلتر در فرآیند جمع آوری داده ها و برای هدف قرار دادن اهداف بر اساس مناطق، کشورها، شهرها، و شماره تلفن ها یا ایمیل ها عمل می کند.

۲. مرکز داده ایرو اسپیس، پایگاه نیروی هوایی در برکلی، کلرادو: اطلاعات جاسوسی جمع آوری شده در ماهواره های ثابت، و سایر فضا پیماها و پست های شنود فرامنطقه ای، به این پایگاه در خارج از دنور فرستاده می شود.

حدود ۸۵۰ کارمند NSA مسئول دنبال کردن فعالیت ماهواره ها، مخابره داده های هدف، و دریافت داده های جدید هستند.

۳. مقر NSA در جورجیا، فورت گوردون، آگوستا: تمرکز این مقر بر روی جاسوسی از اروپا، خاورمیانه و شمال آفریقا است. نام رمز اینجا Sweet Tea (چای شیرین) است که گسترش فوق العاده ای یافته و با ۵۶,۱۱۳ متر مربع مساحت، میزبان ۴,۰۰۰ متصدی، تحلیلگر و دیگر متخصصین اطلاعاتی است.

۴. مقر NSA در تگزاس، پایگاه نیروی هوایی لیک لند، سن آنتونیو: این مرکز با تمرکز بر روی آمریکای لاتین، و سپس از ۱۱ سپتامبر بر روی خاورمیانه و اروپا به کار می پردازد. حدود ۲,۰۰۰ کارمند فعال دارد و NSA به تازگی سرمایه گذاری ۱۰۰ میلیونی برای نوسازی مرکز داده بزرگ آن انجام داده که محل پشتیبان گیری برای مرکز داده یوتا خواهد بود.

۵. مقر NSA هاوایی، اوآهو: این مقر در جریان جنگ جهانی دوم به عنوان یک کارخانه ساخت هواپیما برپا شد، یک مقر زیر زمینی معروف به Hole که ۲۳,۲۲۵ متر مربع مساحت دارد و در طول زمان گسترش یافته ولی حالا ۲,۷۰۰ کارمند آن، به سطح زمین منتقل شده اند و در مقر جدیدی با ۲۱,۳۰۰ متر مربع مساحت، کار می کنند.

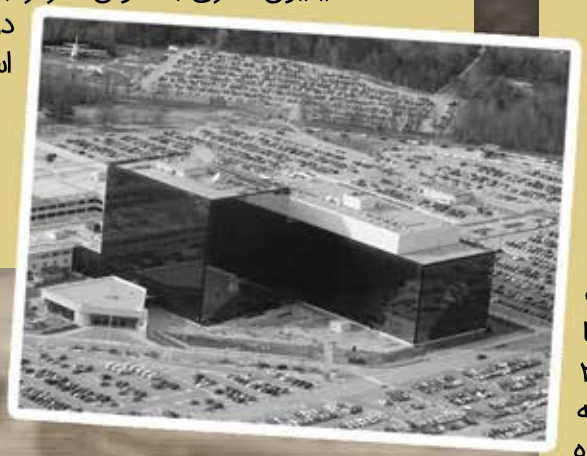
۶.پست های شنود داخل امریکا: NSA همیشه در رصد ارتباطات ماهواره ای بین المللی آزاد بوده ولی بعد از ۱۱ سپتامبر، سوئیچ های مخابراتی را در داخل نیز بر پا کرده تا ترافیک تماس آمریکا را زیر نظر داشته باشد.

۷. پست های شنود خارج از آمریکا: NSA حداقل بر روی ۱۲ تا از شاهراه های ارتباطاتی جهان، سیستم شنود کارگذاشته که هر یک قادر هستند اطلاعات را با سرعت بالا منتقل کنند.

۸. مرکز داده یوتا، بلافدیل: ۲ میلیارد دلار خرج ساخت آن شده تا به عنوان یک پایگاه ذخیره سازی دیجیتال و نیز قلب شبکه ابری NSA فعالیت کند و برای کدگشایی از اسنادی که تا پیش از این غیر قابل بازگشایی بوده اند، به کمک آید.

۹. مرکز پژوهش های چند منظوره، اوک ریج، تنسی: حدود ۳۰۰ دانشمند و مهندس کامپیوتر با درجه های امنیتی بالا در اینجا به سختی کار می کنند. وظیفه شان ساخت سریع ترین ابر کامپیوترها، نوشتن برنامه های رمزگشا و اجرای سایر پروژه های فوق محرمانه است.

۱۰. مقر اصلی NSA، فورت میدل، مریلند: تحلیلگران در این محل بر روی داده های ذخیره شده در یوتا کار خواهند کرد تا گزارش ها و پیشنهادات را آماده ارائه به سیاست گزاران کنند. برای آسان سازی بارگذاری اطلاعات، یک ساختمان ۸۹۶ میلیون دلاری با عنوان "مرکز اَبَر کامپیوتر" نیز دردست ساخت است.



نویسنده:
الهام همتی

آشنایی با جرایم رایانه ای

قسمت دوم

قانون گذار در فصل دوم و سوم جرایم، علیه صحت و تمامیت داده ها و سامانه های مخابراتی را عنوان نموده که عنصر مادی این نوع جرایم را می توان مانند جرایم علیه اموال و مالکیت دانست. قانون گذار در این فصول، جرایمی همچون جعل رایانه ای، تخریب و اخلال در سامانه های رایانه ای و سرقت و کلاهبرداری مرتبط با رایانه را مطرح نموده و حداکثر مجازات را برای جعل رایانه ای، حبس از یک تا پنج سال و جزای نقدی از بیست میلیون ریال تا یکصد میلیون ریال در نظر گرفته است. به نظر می رسد با توجه به اینکه جرایم رایانه ای مانند سرقت و کلاهبرداری رایانه ای ابتدا با جعل یک سایت مشهور شروع می شود، قانون گذار چنین مجازات سنگینی را نسبت به دیگر جرایم در این بخش در نظر گرفته است.

فصل چهارم قانون، به جرایم علیه عفت و اخلاق عمومی پرداخته و مصادیق محتویات مستهجن را بیان نموده است. عنصر مادی این جرایم مانند جرایم علیه عفت عمومی و ماده ۱۰۱ قانون مجازات اسلامی می باشد. حداکثر مجازات در نظر گرفته شده برای اینگونه جرایم، حبس از نود و یک روز تا یک سال و جزای نقدی از پنج میلیون تا بیست میلیون ریال است.

فصل پنجم به مصادیق جرم هتک حیثیت و نشر اکاذیب به وسیله ی سامانه های رایانه ای پرداخته که عنصر مادی اینگونه جرایم مانند مواد ۱۱۳ تا ۳۱۱ قانون مجازات اسلامی می باشد. در فصل ششم مواد ۳۱۳ تا ۳۰۲ قانون مجازات اسلامی، قانون گذار مسئولیت کیفری اشخاص حقیقی و حقوقی مانند شرکت های ارائه دهنده ی خدمات دسترسی را مشخص نموده و عدم تأمین نظر قانون گذار را جرم تلقی و حتی مجازات جزای نقدی تا یک میلیارد ریال و تعطیلی موقت در نظر گرفته است.

از آن جایی که نوع خدمات این گونه شرکت ها نقش به سزایی در کنترل جرایم سایبری دارند و در صورتی که موازین قانونی و اخلاقی را مانند پالایش سایت های غیراخلاقی، رعایت ننمایند، خسارات مادی و معنوی زیادی به جامعه وارد خواهد شد؛ قانون گذار چنین ضمانت اجرایی سنگینی را به نسبت سایر جرایم تعیین نموده است.

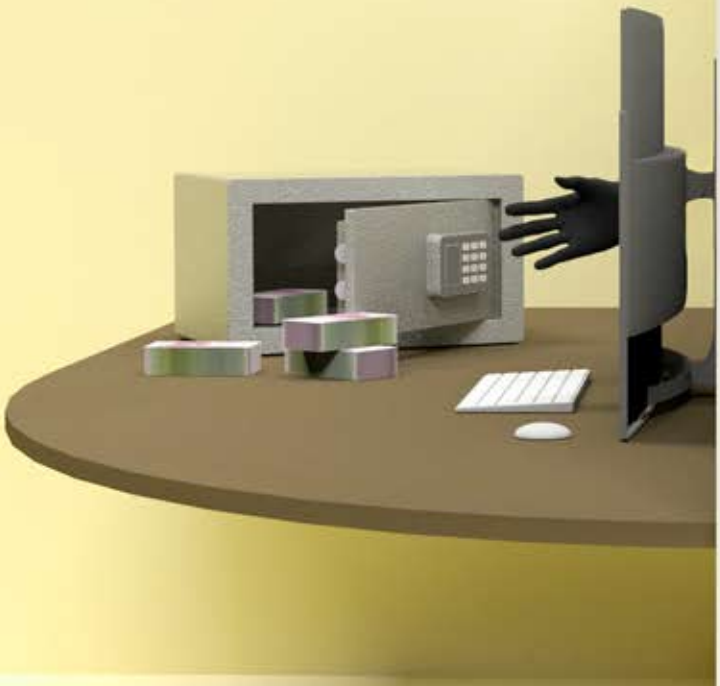
ضمنا در این فصل، قانون کارگروهی را برای بررسی محتوای مجرمانه فضای سایبری تعیین نموده که این کارگروه به ریاست دادستان کل کشور دوبار در ماه تشکیل جلسه می دهد و مصادیق پالایش را رسیدگی می نمایند.

این کمیته وظیفه دارد هر شش ماه در خصوص پرونده ی پالایش محتوای مجرمانه گزارشی را به روسای قوای سه گانه و شورای عالی امنیت ملی تقدیم کند.

در فصل هفتم مواردی مانند توزیع و انتشار ویروس، معامله نرم افزار، آموزش تخریب در سامانه های رایانه ای و مجازات حبس از نود و یک روز تا یک سال و جزای نقدی پنج میلیون ریال تا بیست میلیون ریال پیش بینی شده است.

در فصل هشتم و قسمت آخر بخش یکم، مواردی همچون کارمند دولت یا عضویت نیروهای مسلح یا مقامات قضایی و به طور کلی عضویت رسمی و غیررسمی قوای سه گانه را که به مناسبت انجام وظیفه مرتکب جرم رایانه ای شده اند و نیز تکرار جرم برای بیش از دو بار را جزء تشدید مجازات قلمداد نموده که مرتکب را به بیش از دو سوم حداکثر یک یا دو مجازات مقرر در قانون محکوم می نماید.

در بخش دوم، قانون گذار، آیین دادرسی برخورد با جرایم رایانه ای را مشخص کرده و در ابتدا، اصل سرزمینی بودن و جرایم علیه حاکمیت جمهوری اسلامی را مطرح می کند و در ادامه نحوه ی حفظ ادله ی جرم، تفتیش و توقیف سامانه های رایانه ای را توسط ضابطان و نیز وظایف شرکت های ارائه دهنده ی خدمات اینترنتی را در حفظ داده ها و اطلاعات رایانه ای مشخص می نماید.
ضمنا اینکه ضابطین موظف به رعایت حریم خصوصی افراد بوده و در صورتی که ضابط برابر دستور مقام قضایی عمل نکرده باشد، مجازات های لازم پیش بینی شده است.



می توان گفت در حوزه ی برخورد با جرایم سایبری از نظر قانون مشکل خاصی وجود ندارد، تنها در خصوص برخی از جرایم مانند جرایم علیه عفت و اخلاق عمومی و یا انتشار ویروس رایانه ای، مجازات های خفیفی در نظر گرفته شده که بایستی با توجه به گستردگی این فضا و حجم خسارت هایی که وارد می آید تناسب جرم و مجازات رعایت و در مجازات ها تجدید نظر شود و در آخر می توان به این نکته اشاره کرد که رسیدگی به پرونده های جرایم رایانه ای در تهران و در دادسرای ویژه مبارزه با جرایم رایانه ای صورت می گیرد و امید است با تلاش مسئولن در سایر نقاط کشور نیز راه اندازی دادسراهای مشابه تسری یابد.

یکی از مهم ترین سیاست جنایی ایران در پیشگیری از جرایم رایانه ای بحث قانون گذاری آن در همین حوزه می باشد. قانون گذاری در فضای سایبری را با رویکردی در سه مرحله می توان تبیین کرد. قانون گذاری در روش های حقوق کیفری باید با شناخت به کارگیری فناوری جدید شروع شود و بخش های ویژه به همراه ساختارهای امنیتی انتظامی یا در مفهوم کلی پلیس مورد نیاز می باشند که برای بررسی جرایم سایبری دارای شرایط لازم باشند.
پی ریزی قانون موثر، مقایسه قانون کیفری در قوانین موضوعه با نیازهای برخواسته از انواع جدید تخلفات جنایی ضروری است. در موارد زیادی، قانون های موجود ممکن است بتوانند تغییرات جدید جرایم موجود را بپوشانند.
مرحله ی سوم نگارش قوانین جدید است. براساس تجربه ممکن است برای مراجع قانونی اجراکردن فرآیند نگارش قانون برای جرایم سایبری بدون همکاری بین المللی به دلیل رشد سریع فناوری شبکه و ساختارهای پیچیده آن ها سخت و مشکل است. نگارش قوانین جرایم سایبری به طور جداگانه ممکن است به تعارض قوانین و هدر رفتن منابع منجر گردد و همچنین دنبال کردن توسعه ی استراتژی ها و استاندارد های بین المللی ضروری است. بر همین مبنا می توان گفت تقسیم بندی جرایم رایانه ای از یک سو شامل جرایم علیه اشخاص، علیه اموال و جرایم علیه امنیت و آسایش عمومی و از طرف دیگر جرایم نرم افزار، جرایم داده ها و جرایم علیه حقوق خصوصی فردی می باشند. ازاین رو، به منظور پیشگیری از جرایم رایانه ای سیاست جنایی ایران در بحث قانون گذاری براین است که با تقنین و وضع قوانین در همین حوزه از ارتکاب جرم توسط مجرمان بالقوه و بالفعل پیشگیری نماید.
با رشد جرایم رایانه ای و نوظهور در عصر کنونی پلیس به عنوان یکی از ارکان موثر در سیاست قضایی کشور نسبت به اصلاح و تحول در ساختار سازمانی خود اقدام نموده است و با توجه به این بحث، به منظور ایجاد امنیت در فضای تولید و تبادل اطلاعات ضمن تحول در ساختار امنیتی و انتظامی یعنی تشکیل پلیس فضای تولید و تبادل اطلاعات، براساس دومین راهبرد از سند راهبردی به تصویب هیات وزیران رسید امنیت فضای تولید و تبادل اطلاعات کشور که در تاریخ ۱۳۸۷/۱۲/۰۷ برای نیروی انتظامی جمهوری اسلامی ایران وظیفه ای در نظر گرفته شد.

برگرفته از مقاله «مطالعه ی تطبیقی جرایم سایبری در ایران و حقوق بین الملل»

بلاکچین چیست؟

همه چیز درباره فناوری بلاکچین

قسمت دوم

ویژگی‌های بلاک چین:

در ادامه به ویژگی‌های منحصر به فرد تکنولوژی بلاک چین اشاره خواهیم کرد:

۱.امنیت:

اطلاعات در بلاکچین رمزنگاری شده و سپس ذخیره می شوند، که این امر باعث افزایش امنیت اطلاعات می شود. مسائل مربوط به هش که بیان کردیم نیز در جهت افزایش امنیت است.

۲.شفافیت:

نکته قابل توجه دیگر در بلاکچین این است که اطلاعات برای همه اعضای آن قابل مشاهده است، بنابراین شفافیت در اوج خود قرار دارد (البته در بلاک چین های عمومی و به طور کلی برای اعضایی که مجوز تایید و مشاهده تراکنش‌ها را دارند).

۳. غیر قابل تغییر بودن:

قابلیت جالب دیگر بلاکچین این است که اطلاعات در بلاکچین بدون تائید اکثریت قابل تغییر یا قابل حذف نیست. یعنی اگر اطلاعاتی ثبت شود دیگر تمام است، همه اعضا می‌توانند آن را ببینند، قابل حذف یا تغییر نیست و از امنیت فوق‌العاده بالایی برخوردار است.

بهتر است برای ملموس تر شدن این مطلب مثالی ذکر کنیم. تصور کنید علی می‌خواهد مقداری پول به سینا ارسال کند. ابتدا علی درخواست خود را اعلام می‌کند و این درخواست به شبکه ارسال می‌شود و به شکل تراکنش در می‌آید. به دنبال آن سرویس دهنده‌های شبکه (اعضای شبکه) پیغام علی (تراکنش) را دریافت می-کنند و صحت آن را مورد بررسی قرار می‌دهند که آیا علی این مقدار دارایی دارد یا خیر؟ آیا کلکی سوار کرده است؟ آیا سینایی با آن مشخصات وجود دارد؟ در صورت صحت این درخواست، تراکنش انجام می‌شود و پول علی درblockchain به سینا منتقل می‌شود، بدون اینکه نیاز به بانک یا فرد واسطی باشد. در انتها تمام اطلاعات در بلاک ذخیره می‌شود.

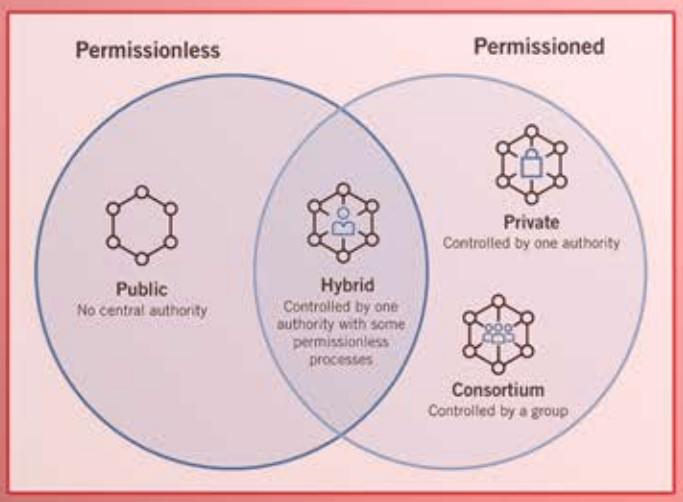
اما نکته جالب‌تر این است که تقریبا همه فکر می کنند تنها کار بلاک چین انتقال ارزهای دیجیتالی مانند بیت کوین و اتریوم و غیره است، اما این تنها یکی از کاربردهای blockchain است. از آنجا که کلمه تراکنش بیشتر در مورد مسائل مالی مطرح می‌شود، شاید باعث شده فکر کنیم که منظور از ثبت تراکنش در بلاک چین تنها تراکنش‌های مالی است.

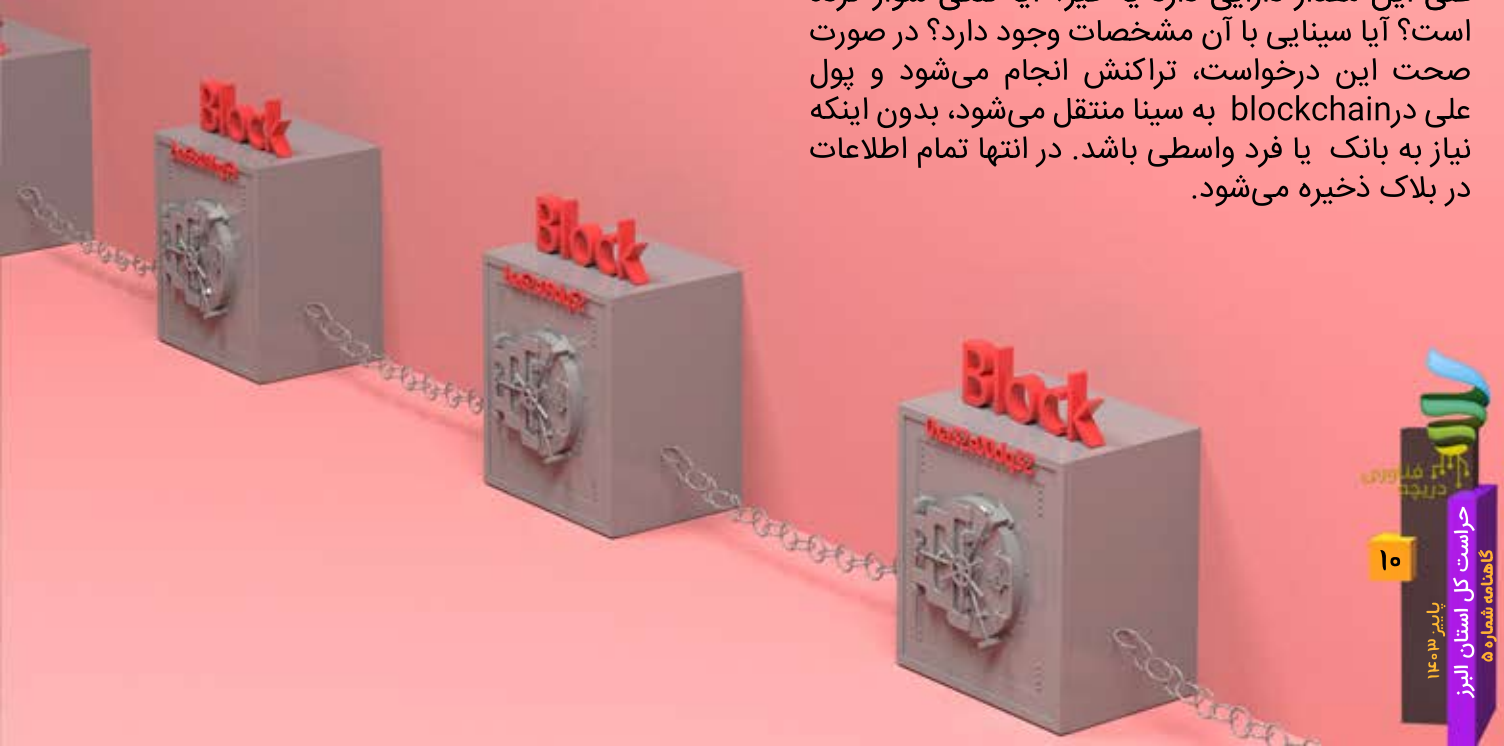
اما در حقیقت اینطور نیست. اگر علی بخواهد حتی متنی برای سینا در شبکه بلاک چین ارسال کند، این عملیات به شکل یک تراکنش ثبت می‌شود. کاربردهای این تکنولوژی همچنان در حال توسعه هستند و حال می توان دید که از این فناوری نوین برای رای گیری شفاف‌تر و بدون تقلب استفاده می‌شود.

کاربردهای تکنولوژی بلاکچین به غیر از ارز دیجیتال چیست؟

امروزه بسیاری از شرکت‌ها نیز به دنبال پاسخ به سوال بلاکچین چیست رفتند و امروزه در حال استفاده از بلاکچین در بخش‌های مختلف کسب و کار خود هستند که در ادامه به معرفی برخی از آن‌ها می پردازیم:

انواع بلاکچین:





تا به اینجای مقاله توانسته‌ایم به یک درک نسبی درباره بلاکچین چیست دست پیدا کنیم. در ادامه توضیح خواهیم داد که blockchain به طور کلی به چند دسته تقسیم می‌شود. بلاکچین‌ها به‌طور کلی به دو دسته بلاکچین‌های بدون نیاز به مجوز (Permissionless) و بلاکچین‌های با مجوز (Permissioned) تقسیم می شوند.

بلاکچین عمومی (Public Blockchain) در دسته بلاکجین‌های بدون نیاز به مجوز و بلاکچین‌های خصوصی (Private Blockchain) و بلاکچین های کنسرسیومی (Consortium Blockchain) در گروه بلاکچین‌های با مجوز قرار می‌گیرند. یک نوع از بلاکچین نیز با نام بلاکچین هیبریدی (Hybrid Blockchain) وجود دارد که برخی از ویژگی‌های بلاکچین بدون مجوز و برخی از ویژگی‌های بلاکچین بامجوز را دارد.

با انواع مختلف بلاکچین آشنا شوید:

۱. بلاکچین عمومی:

شبکه بلاک چین عمومی به بلاکچینی گفته می‌شود که دسترسی به شبکه آن برای عموم آزاد است، کاملا غیرمتمرکز است و همه می‌توانند یکی از اعضای آن شوند. بلاکچین‌های عمومی این امکان را به همه نودها (گره‌ها) می‌دهد که از حقوق برابر برای دسترسی، ایجاد بلوک جدید و اعتبارسنجی در بلاکچین برخوردار باشند.

بلاکچین‌ها عمومی مانند بلاکچین بیت کوین، بلاکچین اتریوم و سایر ارزهای دیجیتالی بیشتر در پروژه رمزارزها به کار گرفته و برای استخراج و تبادل ارزهای دیجیتال استفاده می‌شود.

۲. بلاکچین خصوصی:

بلاکچین خصوصی که بعضی مواقع به آن بلاکچین مدیریت‌شده نیز می‌گویند، توسط سازمان‌ها و نهادهای مشخص کنترل می‌شوند.

در این نوع بلاکچین‌ها قدرت یا گروه بالادستی تصمیم می گیرند که چه کسانی نود یا اپراتور شبکه باشند. بلاک چین های خصوصی تا حدی غیرمتمرکز هستند؛ زیرا دسترسی عمومی به این بلاک چین ها محدود شده است. برخی از نمونه‌های بلاکچین خصوصی شامل شبکه تبادل ارز مجازی کسب وکار به کسب وکار یا B2B ریپل و هایپرلجر می‌شود.

۳. بلاکچین کنسرسیومی:

بلاک چین کنسرسیومی جز بلاکچین‌های بامجوز است. این بلاکچین‌ها برخلاف بلاکچین‌های خصوصی توسط گروهی از سازمان‌ها و نهادها اداره می‌شوند، بنابراین، بلاکچین‌های کنسرسیومی نسبت به بلاکچین‌های خصوصی از تمرکززدایی بیشتری برخوردار هستند و در نتیجه سطوح بالاتری از امنیت را به همراه دارند.

راه‌اندازی بلاکچین کنسرسیومی می‌تواند فرآیندی دشوار باشد، زیرا به همکاری بین تعداد زیادی از سازمان‌ها نیاز دارد. چالش‌های لجستیکی از جمله فراز و نشیب‌های این بلاکچین است. برخی از اعضای زنجیره‌های تامین ممکن است فناوری لازم یا زیرساخت لازم برای پیاده‌سازی بلاک چین را نداشته باشند. گروهی نیز ممکن است تصمیم بگیرند، هزینه‌های اولیه برای دیجیتالی کردن داده‌های خود و اتصال به سایر اعضای زنجیره تامین هزینه بسیار سنگینی است.

۴. بلاکچین هیبریدی:

بلاک چین هیبریدی توسط یک سازمان کنترل می‌شوند، اما دارای سطحی از نظارت هستند (مانند بلاکچین عمومی) که برای اعتبارسنجی تراکنش‌های خاص مورد نیاز است. نمونه ای از بلاکچین هیبریدی IBM Food Trust است که برای بهبود کارایی در کل زنجیره تامین مواد غذایی ایجاد شده است.

نویسنده: حمیدرضا کاوسی

بررسی کاربرد هوش مصنوعی در استراتژی های دفاعی اسرائیل

(قسمت اول)

هوش مصنوعی (AI) به سرعت به عنوان یکی از متحول کننده‌ترین فناوری‌های دیجیتال ظاهر شد و سیاست‌های حمایتی دولت و سرمایه‌گذاری در پروژه‌های تحقیق و توسعه در کنار فرهنگ نوآورانه، بستر مناسبی را برای رشد و پیشرفت این فناوری فراهم کرده‌اند. اسرائیل به عنوان یکی از پیشگامان جهانی در حوزه فناوری و نوآوری، به ویژه در زمینه‌های امنیت سایبری و دفاعی، جایگاه ویژه ای در استفاده از هوش مصنوعی دارد. اسرائیل نه تنها با بهره‌گیری از دانشگاه‌ها و مراکز تحقیقاتی معتبر، بلکه از طریق همکاری‌های نزدیک با شرکت‌های فناوری، به توسعه و پیاده‌سازی راه‌حل‌های هوش مصنوعی پرداخته است. افزایش استفاده از AI در بخش‌های مختلفی مانند بهداشت، حمل و نقل و کشاورزی نیز نمایانگر این است که اسرائیل به دنبال گسترش دامنه تأثیرات هوش مصنوعی فراتر از مرزهای نظامی می‌باشد.

بمباران نظامی ۱۱ روزه غزه در ماه مه ۲۰۲۱ حتی توسط نیروهای دفاعی اسرائیل (IDF) «نخستین جنگ هوش مصنوعی» نامیده شد. در حمله کنونی به غزه، ما شاهد استفاده اسرائیل از سه دسته وسیع از ابزارهای هوش مصنوعی هستیم:

سیستم‌های تسلیحاتی مرگبار (LAWS) و سلاح‌های نیمه خودکار: ارتش اسرائیل در استفاده از کوادکوپترهای کنترل از راه دور مجهز به مسلسل و موشک برای نظارت، وحشت و کشتن غیرنظامیانی که در چادرها، مدارس پناه گرفته‌اند، پیشگام بوده است.

بیمارستان ها و مناطق مسکونی ساکنان کمپ آوارگان نصیرات غزه گزارش می دهند که برخی پهپادها صدای گریه نوزادان و زنان را پخش می کنند تا فلسطینیان را فریب دهند و هدف قرار دهند. سال هاست اسرائیل پهپادهای انتحاری، تک‌تیراندازهای روبو و برجک‌های مجهز به هوش مصنوعی را برای ایجاد «مناطق کشتار خودکار» در امتداد مرز غزه مستقر کرده است و در سال ۲۰۲۱، یک ربات نظامی نیمه خودمختار را نیز مستقر کرد. "جگوار" به عنوان یکی از اولین ربات های نظامی در جهان که می تواند جایگزین سربازان در مرزها شود، معرفی شد.

سیستم‌های تشخیص چهره و نظارت بیومتریک: تهاجم زمینی اسرائیل به غزه، فرصتی برای گسترش نظارت بیومتریک خود از فلسطینی‌ها بود که قبلاً در کرانه باختری و بیت‌المقدس شرقی مستقر شده بودند. نیویورک تایمز گزارش داد که چگونه ارتش اسرائیل از یک سیستم تشخیص چهره گسترده در غزه برای نظارت گسترده در غزه، جمع‌آوری و فهرست‌بندی چهره‌های فلسطینی‌ها بدون اطلاع یا رضایت آن ها استفاده می‌کند. بر اساس این گزارش، این سیستم از فناوری شرکت اسرائیلی Cor-sight و Google Photos برای تشخیص چهره‌ها در میان جمعیت استفاده می‌کند.

سیستم‌های تولید هدف خودکار: مهم‌ترین آن ها «The Gospel» (گاسپل: در مسیحیت به معنای بشارت) است که اهداف زیرساختی را تولید و برای تخمین تعداد تلفات غیرنظامیان در بمباران، پیشنهاد مناسب‌ترین اهداف برای حمله و محاسبه مقدار مهمات مورد نیاز بهره می‌برد.

دیگری Lavender است که به معنی اسطوخودوس می باشد و برای ردیابی و هدف قرار دادن شبه‌نظامیان مظنون (حماس یا جهاد اسلامی فلسطین) زمانی که با خانواده هایشان در خانه هستند، طراحی شده است. سازندگان این نرم‌افزار مدعی هستند که لاوندر با دقت ۹۰ درصد می تواند افراد را شناسایی کند.

در جنگ‌های اخیر و تنش‌های بین اسرائیل و ایران، استفاده از هوش مصنوعی به طور فزاینده‌ای مورد توجه قرار گرفته است و در مجموع می توان گفت، هوش مصنوعی به عنوان یک ابزار کلیدی در استراتژی‌های نظامی اسرائیل در تقابل با ایران به کار گرفته شده و نشان‌دهنده تحولی در روش‌های جنگی مدرن است. این مقاله به بررسی کاربرد هوش مصنوعی در استراتژی های دفاعی اسرائیل می پردازد.

برخی از جنبه‌های استفاده اسرائیل از هوش مصنوعی در این درگیری‌ها شامل موارد زیر است:

۱. شناسایی و جمع‌آوری اطلاعات: اسرائیل از الگوریتم‌های هوش مصنوعی برای تجزیه و تحلیل داده‌ها و شناسایی نقاط لحظه‌ای در نقاط مختلف ایران استفاده می‌کند. این شامل تصاویر ماهواره‌ای، داده‌های الکترونیکی و اطلاعات جاسوسی است که می‌تواند به شناسایی تهدیدها کمک کند.

۲. سیستم‌های تسلیحاتی پیشرفته: اسرائیل در حال توسعه سیستم‌های تسلیحاتی است که قادرند به طور خودکار به تهدیدات پاسخ دهند. این سیستم‌ها می‌توانند تصمیمات سریع‌تری بگیرند و به راحتی تهدیدات را شناسایی و هدف قرار دهند.

۳. مدیریت جنگ‌افزار:
استفاده از الگوریتم‌های هوش مصنوعی برای بهینه‌سازی مدیریت جنگ‌افزارها و انتخاب اهداف ممکن به تهدیدات پیچیده‌ای که ایران ایجاد کرده است، کمک می‌کند.

٤. عملیات سایبری: هوش مصنوعی در جنگ‌های سایبری برای شناسایی آسیب‌پذیری‌ها و حملات پیشرفته استفاده می‌شود. اسرائیل توانسته است با استفاده از هوش مصنوعی به صورت پیشگیرانه به تهدیدات سایبری مقابله کند.

٤. عملیات سایبری: هوش مصنوعی در جنگ‌های سایبری برای شناسایی آسیب‌پذیری‌ها و حملات پیشرفته استفاده می‌شود. اسرائیل توانسته است با استفاده از هوش مصنوعی به صورت پیشگیرانه به تهدیدات سایبری مقابله کند.

۵. تحلیل رفتار دشمن: با تجزیه و تحلیل الگوهای رفتاری و سیستم‌های ارتباطاتی نیروهای ایرانی، اسرائیل می‌تواند پیش‌بینی کند که چگونه و چه زمانی ایران ممکن است اقدام کند. این فناوری به ارتش اسرائیل کمک می‌کند تا اطلاعات دقیق‌تری درباره تهدیدات احتمالی کسب کند.

اسرائیل در جنگ و تنش‌های اخیر خود با ایران از مجموعه ای از ابزارهای پیشرفته شناسایی و نظارت استفاده کرده است. این ابزارها به ارتش اسرائیل کمک می‌کنند تا اطلاعات دقیقی از فعالیت‌های ایران و نیروهای وابسته به آن به دست آورد. احتمال می رود برخی از این ابزارها به شرح ذیل باشند:

۱. ماهواره‌های نظامی: اسرائیل دارای یک برنامه فضایی قوی است که شامل ماهواره‌های شناسایی و تجسسی است. این ماهواره‌ها قادر به تصویربرداری با وضوح بالا و جمع‌آوری اطلاعات در مورد فعالیت‌های نظامی و زیرساخت‌های مهم ایران هستند. ماهواره‌های نظامی اسرائیل یکی از ارکان کلیدی استراتژی‌های اطلاعاتی و نظامی این کشور در برابر ایران و تهدیدات دیگر را تشکیل می‌دهند. این ماهواره‌ها به جمع‌آوری اطلاعات در زمان واقعی، شناسایی تهدیدات و تجزیه و تحلیل وضعیت نظامی کمک می‌کنند. در این‌جا به بررسی جزئیات و انواع ماهواره‌های نظامی اسرائیل و نقش آن‌ها در جنگ با ایران می‌پردازیم:

۱.۱. انواع ماهواره‌های نظامی اسرائیل:

الف) ماهواره‌های شناسایی و تجسسی:

- **ماهواره‌های اوفک (Ofek):** این ماهواره‌ها به عنوان ماهواره‌های شناسایی الکترونیکی و تصویر برداری به‌کار می روند. آنها قادر به تصویربرداری از زمین با وضوح بالا هستند و برای رصد فعالیت‌های نظامی و زیرساخت‌های حیاتی در ایران و دیگر کشورها استفاده می‌شوند.
- **ماهواره‌های هارون (Haroont):** این ماهواره‌ها به‌ویژه در شناسایی اهداف از پیش تعیین‌شده در مناطق حساس و استراتژیک مؤثرند. آن ها می‌توانند تصاویر با کیفیت بسیار بالا و داده های مربوط به فعالیت‌های نظامی را جمع‌آوری کنند.

ب) ماهواره‌های ارتباطی:

- **ماهواره‌های صیاد (Tahal):** این ماهواره‌ها به‌منظور بهبود ارتباطات نظامی، به خصوص در میدان جنگ و ارتباط با نیروهای ویژه مورد استفاده قرار می‌گیرند.

-ماهواره‌های مخابراتی: این ماهواره‌ها ارتباطات داده و اطلاعات را برای نیروهای نظامی اسرائیل تضمین می‌کنند و می‌توانند در شرایط بحرانی و جنگی اطلاعات حیاتی را انتقال دهند.
ویژگی‌ها و قابلیت‌های این ماهواره ها عبارتند از:
- تصویربرداری با وضوح بالا: ماهواره‌های اسرائیلی می توانند تصاویری با جزئیات دقیق از مناطق مختلف تهیه کنند. این قابلیت به تحلیل‌گران اطلاعاتی اجازه می‌دهد تا تحرکات روزانه و فعالیت‌های نظامی را زیر نظر بگیرند.
-شناسایی حرکات و فعالیت‌ها: ماهواره‌ها با استفاده از سنسورهای حرارتی و راداری می‌توانند حرکات مستمر نیروها، تجهیزات نظامی و تاسیسات ایران را شناسایی و تجزیه و تحلیل کنند.
- پوشش ۲۴ ساعته: با وجود چندین ماهواره در مدار، اسرائیل قادر است به اطلاعات روزانه و ۲۴ ساعته دسترسی پیدا کند که این امر برای تصمیم‌گیری‌های سریع و مؤثر در عملیات نظامی اساسی است.
۲) تکنولوژی‌های شنود الکترونیکی: جمع‌آوری اطلاعات از طریق شنود مکالمات و ارتباطات الکترونیکی، به اسرائیل این امکان را می‌دهد که در مورد برنامه‌های نظامی و تحرکات دشمن آگاهی پیدا کند. تکنولوژی شنود الکترونیکی (SIGINT) یکی از ابزاری است که اسرائیل در جنگ و تنش های خود با ایران به‌طور گسترده‌ای از آن استفاده کرده است. این تکنولوژی شامل جمع‌آوری و تحلیل اطلاعات از انواع ارتباطات الکترونیکی برای درک دقیق‌تر از فعالیت‌ها، برنامه‌ها و تحرکات دشمن است. در اینجا به تفصیل به جنبه های مختلف این تکنولوژی اشاره می‌کنیم:

۲-۱- روش‌های جمع‌آوری اطلاعات:

شنود مکالمات تلفنی: اسرائیل سیستم‌های پیچیده‌ای برای شنود مکالمات تلفنی دارد که به آن‌ها اجازه می‌دهد تا مکالمات عمومی و خصوصی را رصد کنند. این سیستم ها می‌توانند به‌طور خودکار شماره‌های هدف را هدف قرار دهند و تمامی مکالمات را ضبط کنند.
- شنود ارتباطات اینترنتی: با توجه به رشد روزافزون ارتباطات دیجیتال، اسرائیل به جمع‌آوری اطلاعات از طریق پیام‌های فوری، ایمیل‌ها و ارتباطات شبکه‌های اجتماعی نیز توجه کرده است.
این امر شامل تجزیه و تحلیل ترافیک اینترنتی و استفاده از نرم‌افزارهای پیشرفته برای شناسایی فعالیت‌های مشکوک است.
- میکروفن‌های مخفی و ابزارهای نظارت: در برخی مواقع، اسرائیل از میکروفن‌های مخفی و تجهیزات نظارت فیزیکی برای ضبط صداها و فعالیت‌های مشکوک در مناطق مورد نظر استفاده می‌کند.

۲-۲-تحلیل و پردازش داده‌ها:

- الگوریتم‌های یادگیری ماشین: استفاده از تکنیک‌های یادگیری ماشین برای شناسایی الگوها و رفتارهای معمول در مکالمات و پیام‌ها. این الگوریتم‌ها می‌توانند به‌طور خودکار داده‌های دریافتی را تحلیل کرده و اطلاعات مهم را استخراج کنند.
- تجزیه و تحلیل متن: نرم‌افزارهای پیشرفته قادر به تحلیل محتوای متنی و شناسایی نکات کلیدی و موضوعات مهم در مکالمات یا پیام‌ها هستند.
- فلوچارت‌ها و نمودارهای شبکه: تحلیل شبکه‌های ارتباطی برای درک بهتر ارتباطات بین افراد و نهادها و شناسایی ساختارهای خریداری شده و نفوذ مخفی در گروه‌های نظامی یا تروریستی.
۳. سیستم‌های راداری: سیستم های راداری به شرح ذیل می باشد:

۳-۱-رادارهای دوربرد:

-رادارهایAN/TPS-۷۷: این رادارها قابلیت شناسایی و ردیابی هواپیماها و موشک‌ها در فواصل طولانی را دارند و می‌توانند به‌طور همزمان چندین هدف را تحت نظر قرار دهند.
- رادارهای فازواره (Phased Array Radar): این نوع رادارها به‌طور خاص برای شناسایی تهدیدات هوایی و موشکی طراحی شده‌اند و می‌توانند به سرعت و با دقت بالا هدف‌ها را شناسایی کنند.

۳-۲-رادارهای شناسایی و جمع‌آوری اطلاعات:

-رادارهایIntelligence, Surveillance, and Recon-naissance) ISR): این رادارها به جمع‌آوری اطلاعات اطلاعاتی، شناسایی و نظارت در میدان جنگ کمک می کنند و توانایی شناسایی اهداف متحرک و ثابت را دارند.

نسخه نویسی الکترونیکی

قسمت دوم

بر اساس مطالعات انجام شده نمونه هايي از مشكلات نسخه نويسي كاغذي كه موجب به خطر افتادن ايمني بيمار و تأثير منفي بر نتيجه درمان دارويي مي گردند، به شرح زير است:
بروز اشتباه در نام، دوز، دوره درمان، فرمول و ماده مؤثر دارو، دستورالعمل مبهم و نامشخص، دستورات دارويي تلفني يا شفاهي نامفهوم، صدور نسخه براي بيمار اشتباه، مفقود شدن داده هاي بيمار و نسخه نويسي، بالا بودن ميزان جعل در نسخه نويسي و تحميل هزينه ها به داروخانه، دوباره كاري در نوشتن نسخه در مطب پزشكان و داروخانه، سوابق ناقص دارويي بيمار، درمان هاي دارويي تكراري، نقص در ارتباط به دليل دست خط ناخوانا، ابزار ضعيف مديريت تداخلات دارويي، ميزان بالاي عوارض ناخواسته داروها، مشكل بودن انتخاب دارو براي درمان به دليل تنوع، فراواني محصولات دارويي، تفسير نادرست نسخه ها، بالا بودن هزينه هاي بررسي نسخه.
سيستم نسخه الكترونيكي به سيستم های اطلاعاتی در سازمان های مراقبت های بهداشتی مانند بیمارستان ها، مراکز مراقبت های بهداشتی و داروخانه ها متصل می شود. اجرای آن می تواند بر بسیاری از مشکلات فرآیند نسخه نویسی کاغذی غلبه کند و مزایایی از جمله صرفه جویی در هزینه، کاهش خطاهای نسخه، افزایش خوانایی نسخه، بهبود نتایج درمان دارویی، دسترسی الکترونیکی به اطلاعات دارویی و سابقه دارویی بیمار را به همراه خواهد داشت.

نسخه نویسی الکترونیک با توجه به نیازهای داخلی هر کشور طراحی و اجرا می شود و استانداردهای مختلفی نیز برای بهتر شدن آن هر ساله ایجاد می شود. این سیستم نماینده سیستم‌های اطلاعات اجتماعی-فنی چند رشته‌ای است که دارای دامنه وسیع، تخصص‌های مختلف، پیچیدگی‌های متعدد و زیرسیستم‌های متنوع، فرآیند پیاده‌سازی متمایز و راه‌حل‌های فنی خاص در هر کشور است. پزشکی مهم ترین بخش درمان است و تجویز و مصرف دارو یکی از ارکان مهم نظام سلامت در هر کشور است.
امروزه ضرورت استفاده از سیستم‌های نسخه‌نویسی الکترونیکی با توجه به مزایای فراوانی که دارند، بیش از پیش احساس می‌شود. به منظور طراحی و پیاده سازی سیستم های نسخه نویسی الکترونیکی توجه به موارد زیر ضروری می باشد:
-زیرساخت های حقوقی سامانه های نسخه الکترونیکی (تصویب قانون نسخه الکترونیکی، تصویب قانون انتقال، صدور نسخه الکترونیکی داروهای کنترل شده، صدور نسخه کاغذی در صورت نیاز، قانونی بودن امضای الکترونیکی نسخه، رضایت بیمار از مشارکت در این خدمات، و رضایت بیمار برای دسترسی ذینفعان به اطلاعات مورد نیاز)
- پذیرش نسخه از کشورهای دیگر (ارائه نسخه فکس، کاغذی و الکترونیکی، تصویب قوانین تجویز، محدودیت ها)

- معماری سیستم نسخه نویسی الکترونیکی (نوع معماری، پایگاه ملی نسخه های الکترونیکی، پایگاه اطلاعات جمعیتی بیمار، پایگاه ملی پزشکی، پرونده الکترونیک سلامت ملی، مشخصات پزشکی الکترونیک شخصی، اینترنت، شبکه ملی اختصاصی سلامت، شبکه ملی نسخه الکترونیکی، پورتال ملی سلامت)
- مسئولیت سامانه الکترونیک نسخه نویسی (هماهنگی و راهبری سلامت الکترونیک، تامین مالی، ایجاد و نگهداری بانک ملی نسخه الکترونیکی، پیاده سازی پرتال ملی سلامت)
- شناسه های سیستم الکترونیکی نسخه (شناسه ملی بیمار، شناسه دارو، شناسه پزشک، فناوری تایید هویت تجویز کننده و توزیع کننده، شناسه منحصر به فرد نسخه (PUID)، شناسه داروخانه).

اجرای طرح نسخه نویسی الکترونیکی همانند طرح های دیگر ممکن است با چالش‌ها و مشکلاتی همراه باشد. البته بعضی از مشکلات و چالش‌ها تاکنون برطرف شده است، اما بعضی موارد به راحتی قابل برطرف شدن نیستند و نیاز به زمان و مدیریت صحیح‌تر دارند. مهم‌ترین چالش‌ها و مشکلات فعلی نسخ الکترونیک شامل موارد زیر است:

- کندی و قطعی سامانه که باعث شده است تا بیماران نتوانند نسخه خود را دریافت کنند. البته در مواردی که پزشک به صورت الکترونیکی نسخه را صادر کرده و سیستم داروخانه قطع بوده است، بیمار چاره ای جز مراجعه به داروخانه دیگر نداشته است. در حقیقت باید گفت که از مهم‌ترین دلایل این اتفاق، نبود زیرساخت لازم است.
- حفظ اطلاعات بیمار یکی از دغدغه های افراد در این حوزه بوده است. اینکه فردی از جمله پزشک داروخانه یا کارمندان آن جا از اطلاعات بیمار برای هدفی خاص سوء استفاده نکنند. در این خصوص تدابیری اندیشه شده است و مشکلی از این بابت وجود ندارد؛ اما به هر حال لازم است به روزرسانی هایی در این حوزه انجام شود.

Osmani, F., Arab-Zozani, M.,- Shahali, Z., & Lotfi, F. (2023, May). Evaluation of the effectiveness of electronic prescription in reducing medical and medical errors (systematic review study). In Annales Pharmaceutiques Françaises (Vol. 81, No. 3, pp. 433-445). Elsevier Masson.

Samadbeik M, Ahmadi M. Electronic Prescription System: Concepts and Standards. Health Inf Manage 2013; 10(2): 1-13.

سازمان حراست کل کشور
حراست کل استان البرز

بدینوسیله از کلیه همکاران شاغل در استان البرز
دعوت می شود
مقالات خود را از طریق پست الکترونیکی و یا آی دی شبکه های اجتماعی اعلام شده ذیل
جهت چاپ در نشریه دریچه فناوری ارسال نمایند.

محورهای مقالات :

- هوش مصنوعی
- سیستم های هوشمند
- سیستم های چند رسانه ای
- رباتیک
- امنیت تبادل اطلاعات
- اپلیکیشن ها
- امنیت و شبکه
- امنیت اطلاعات
- رایانش ابری
- واقعیت مجازی
- فناوری های نوین
- مدیریت سیستم های اطلاعاتی
- فناوری اطلاعات و ارتباطات
- فناوری اطلاعات و سلامت
- شبکه های اجتماعی
- شبکه های کامپیوتری
- آینده پژوهی امنیت سایبری در ایران
- آینده پژوهی در فناوری اطلاعات و ارتباطات
- آموزش الکترونیک
- مهندسی نرم افزار
- و سایر زمینه های مرتبط با حوزه فناوری اطلاعات

@daricheh_fannavari
پست الکترونیک: daricheh1401fannavari@chmail.ir شماره تماس: ۰۲۶۳۴۱۸۹۶۱۰

بسم الله الرحمن الرحیم

دانش سلطنت و قدرت است. هر که آن را بیابد با آن یورش برد و پیروز شود و هر که آن را نیابد بر او یورش برند و مغلوب گردد.

امام علی (ع)

سازمان حراست کل کشور
حراست کل استان البرز

فناوری دریچه