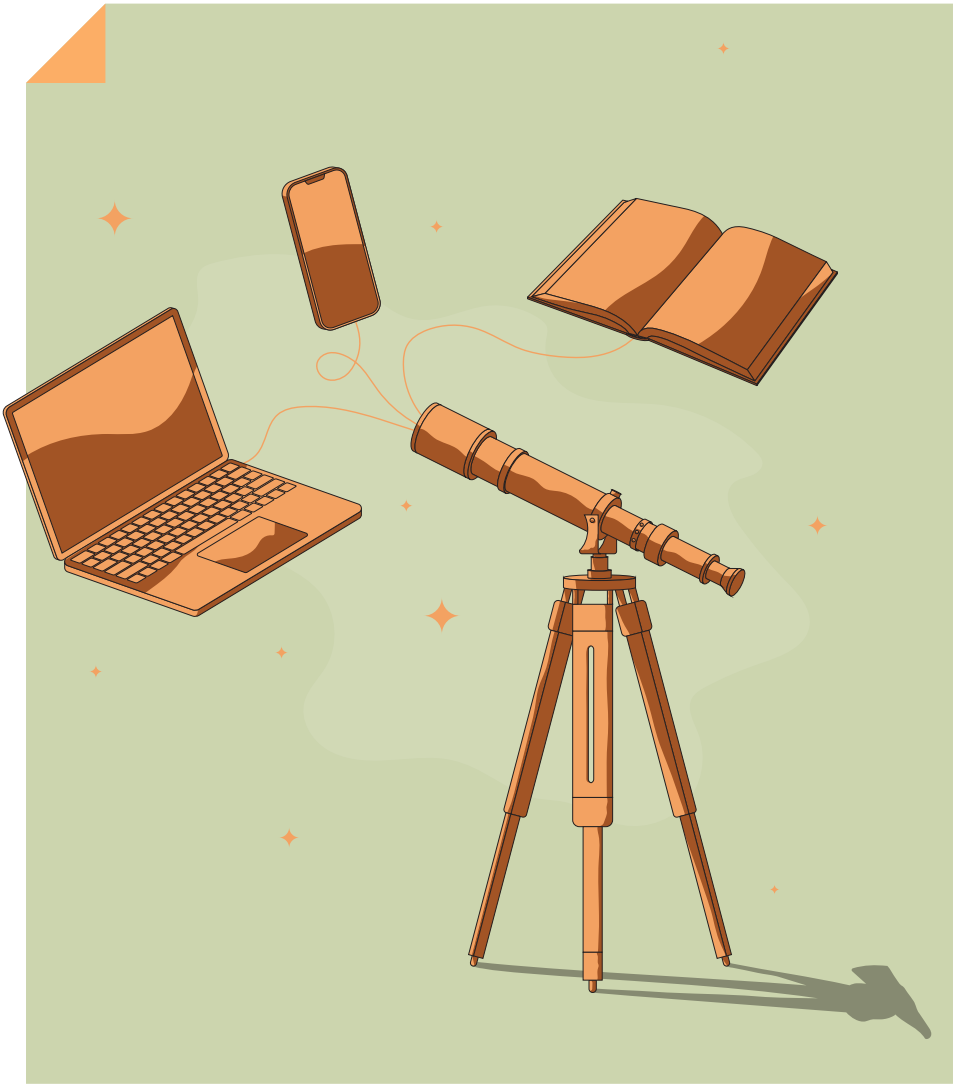
زاویه
نگاهی نو؛
به حکمرانی فضای مجازی



رصدنامه حکمرانی سایبری

مروری بر اندیشکده‌های شاخص جهان | آذر ۱۴۰۱

دوره اول
شماره ۶

دوره ۱، شماره ۶، آذر ۱۴۰۱

رصدنامه حکمرانی سایبری

مروری بر اندیشکده‌های شاخص جهان

تهیه‌وتنظیم
حسین دهقانیان‌پور
ناظر علمی
احسان امینی باغبادرانی
مدیر مطالعه
امین زاده‌حسین

نشانی
تهران، ضلع غربی میدان فلسطین،
خیابان آیت‌الله طالقانی، پلاک ۳۹۷
تلفن
۰۲۱-۸۶۰۵۴۲۹۱
وبسایت
www.sccm.ir

برای دسترسی به منبع اخبار (در نسخه دیجیتال)
کافی است روی بارکد پایین صفحات
لمس/کلیک کنید.

محتوای این گزارش لزوماً منعکس‌کننده دیدگاه
مجموعه زاویه و مرکز راهبردی فرهنگ و رسانه نیست.

مقدمه

اندیشـکده‌های شـاخص جهان به جهت تعییـن الگو و ارائه خط‌مشـی در حـوزه حکمرانی فضای مجازی به تصمیم‌سـازان، اطـلاع از جزئیـات تحـولات جاری حکمرانـی فضای مجـازی، پالایش و بومی‌سـازی محتوای اندیشـکده‌های جهـان متناظر با نیازهـای داخـل کشـور و...، نهادهای علمـی و راهبـردی حائز اهمیت و برجسـته‌ای به شـمار می‌رونـد. بر همین مبنـا، لزوم توجـه به محتـوای تولیدی از سـوی این مراکـز مطالعاتی، امری ضروری اسـت.

فرایند تهیه گزارش رصد اندیشکده‌ها، با شناسایی و گزینش بیش از ۴۰ مرکز مطالعاتی برتر در سطح جهان، آغاز شد. انتخاب اندیشکده‌ها براساس گزارش سالانه دانشگاه «پنسیلوانیا» از اندیشکده‌های برتر جهان صورت پذیرفت؛ علاوه بر این، اندیشکده‌هایی که در حوزه فضای مجازی فعالیت دارند نیز در فرایندی دقیق، ارزیابی و انتخاب شدند. در گزارش رصد اندیشکده‌ها ۳۰ اندیشکده آمریکایی و حدود ۱۱ اندیشکده از کشورهای دیگر ازجمله انگلستان، چین، هلند، دانمارک، هند، ژاپن، آلمان، برزیل و .... مورد بررسی قرار می‌گیرند. اهم اندیشکده‌ها که بیشترین مقالات و گزارش‌ها از آن‌ها استخراج شده به تفکیک اندیشکده‌های آمریکایی و غیرآمریکایی در پایین آمده است:

اهم‌اندیشکده‌های‌آمریکایی

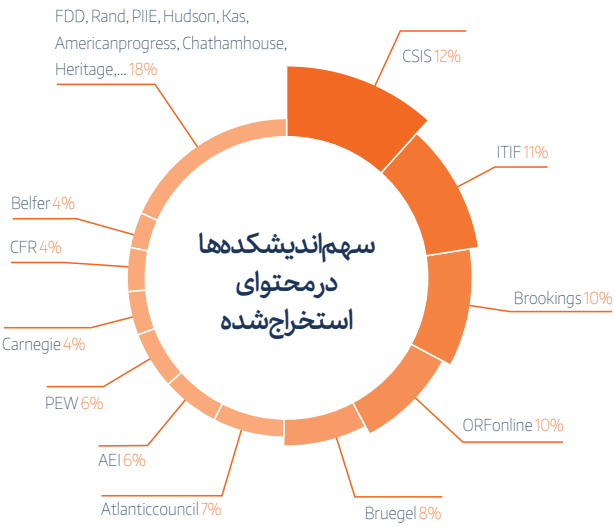
- امریکن‌اینترپرایز
- بروکینگز
- هریتیج
- شورای‌آتلانتیک
- بِلفِر
- رَند
- کارنگی
- پیو
- ویلسون
- شورای‌روابط خارجی
- موسسه‌اقتصادبین‌الملل‌پیترسون
- موسسه‌هادسون
- مرکزمطالعات‌استراتژیک‌وبین‌المللی‌و...

اهم‌اندیشکده‌های‌غیرآمریکایی

- چتم‌هاوس
- بروگل
- موسسه‌امور بین‌الملل‌واروپا
- بنیادفناوری‌اطلاعات‌ونوآوری
- مرکزمطالعات‌سیاست‌اروپاو...

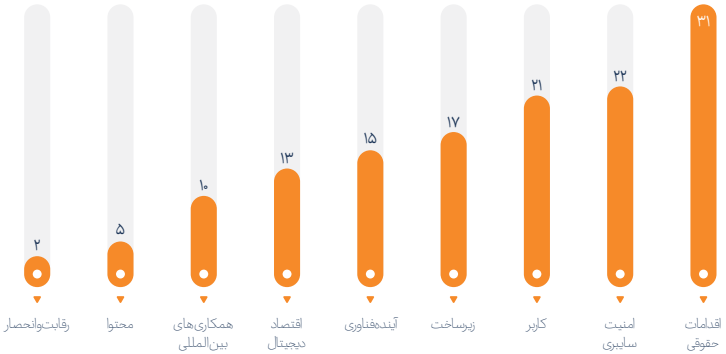
در این شماره از رصد که در بازه یک‌ماهه آذر نگارش شده است، ۱۳۷ عنوان استخراج شد که شامل گزارش، رویداد مجازی، یادداشت، پروژه‌های تحقیقاتی و... می‌شود.

باتوجه به نمودار بالا، مرکز مطالعات استراتژیک و بین‌المللی «CSIS» با ۱۲ درصد بیشترین محتوای تولیدی مرتبط با فضای مجازی را به خود اختصاص داد و بعد از آن بنیاد نوآوری و فناوری اطلاعات «ITIF» با ۱۱ درصد، بروکینگز «Brookings» و بنیاد آبزِرور «ORFonline» هرکدام با ۱۰ درصد، رَند «Rand» و کارنگی «Carnegie» هرکدام با ۱۰ درصد، و بنیاد تحقیقاتی آبزِروِر «Orfonline» هرکدام با ۸ درصد، بروگل «Bruegel» با ۷ درصد، امریکن اینترپرایز «AEI» و مرکز افکار سنجی پیو «PEW» هرکدام با ۶ درصد، کارنگی «Carnegie» و شورای روابط خارجی «CFR» هرکدام با ۴ و سایر اندیشکده‌ها، مشترکاً در تولید ۱۸ درصد از محتوا، سهیم بوده‌اند.



مطالب مستخرج، طبق یک طبقه‌بندی موضوعی که از پیش تعیین شده بود؛ در دسته‌های محتوا، اقدامات حقوقی، رقابت و انحصار، آینده فناوری، کاربر، اقتصاد دیجیتال، زیرساخت، امنیت سایبری و همکاری‌های بین‌المللی تقسیم شدند که فراوانی مطالب هر دسته موضوعی به شرح ذیل است:

سهم موضوعات فناوری در محتوای اندیشکده‌ها



هفتادوچهار عنوان انتخابی از اندیشکده‌های شاخص جهان در آبان‌ماه، دربرگیرنده بیش از ۴۰۰ هزار کلمه محتوا می‌باشد که توسط ۳۵۰ اندیشمند تولید و نگارش شده‌اند. محتوای استخراج‌شده شامل متن رویدادهایی که در گذشته برگزار شده‌اند، گزارش‌ها، آمارها، یادداشت‌ها و مقالات علمی هستند.

در ادامه به بررسی ۷۴ عنوان برگزیده از ۱۳۷ گزارش استخراج شده پرداخته شده است.

گزارش‌های برگزیده

چهار سناریو درباره آینده توییتر

در این مقاله، چهار سناریو برای آینده توییتر تجزیه‌وتحلیل می‌شود:

۱. ورشکستگی

یکی از مهم‌ترین عوامل در تعیین آینده مالی توییتر، تبلیغ‌کنندگان هستند، زیرا بخش عمده‌ای از درآمد این شرکت از تبلیغات است. اگر بسیاری از حامیان مالی مخارج خود را متوقف کنند، این حرکت به‌سرعت می‌تواند پلتفرم توییتر را نابود کند. از دست دادن درآمدهای قابل‌توجه می‌تواند حفظ خدمات اولیه یا به‌روزرسانی این پلتفرم را دشوار کند.

۲. محتوای معتدل اندک؛ افراط‌گرایی زیاد

ایلان ماسک درمورد علاقه خود به ترویج آزادی بیان و اجازه دادن به طیف وسیع‌تری از محتوا در توییتر صحبت کرده است و به‌عنوان نشانه‌ای از تعهد خود به این چشم‌انداز، دونالد ترامپ، کتی گریفین، بابیلون بی و جردن پیترسون را به سکو بازگردانده است. هرکدام از این افراد به دلایل مختلف، از شعارهای تحریک‌آمیز و جعل هویت گرفته تا ترنس‌هراسی، تعلیق شده بودند که بازگشت آن‌ها می‌تواند سبب زیادشدن محتوای افراطی در این پلتفرم شود.

۳. مشکلات فنی در نگهداری سایت

استعفا و پایان کار بسیاری از مهندسان و کارکنان به این معنی است که حفظ زیرساخت‌های فنی و محافظت از پلتفرم در برابر حریم خصوصی و همچنین تهدیدات امنیت سایبری برای توییتر دشوار است. تعجیل در بازنویسی کدهای نرم‌افزاری با دقت پایین و تجربه محدود، ممکن است این پلتفرم را در معرض کلاهبرداری‌های مجرمانه، هک‌های امنیت سایبری و یا تهدیدات باج‌افزار قرار دهد.

۴. بقا ازطریق خدمات ممتاز

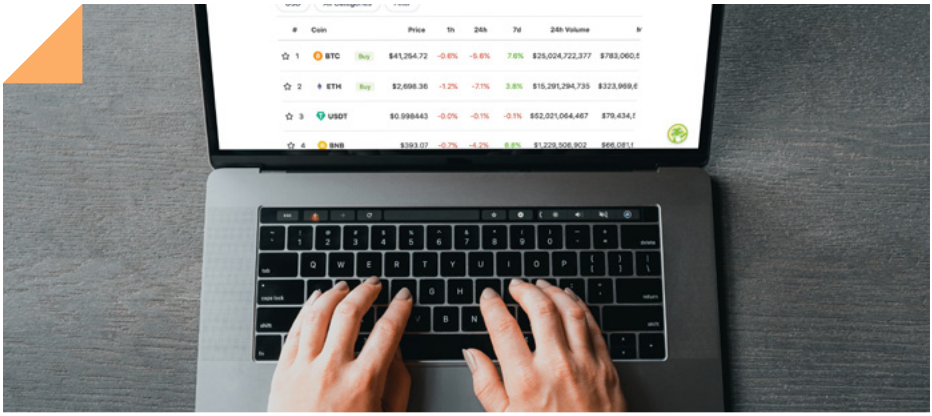
بااین‌حال، شروع پر از چالش ماسک، شکست را تضمین نمی‌کند. بسیاری از سازمان‌ها دوران سختی را پشت سر گذاشته‌اند، اما موفق شده‌اند با نوآوری در ارائه خدمات و محصولات جدید طی درازمدت پیشرفت کنند. توییتر نیز علی‌رغم کاهش هزینه‌ها و استعفای کارکنان، همچنان می‌تواند با عرضه محصولات جدید پرکاربرد و جذب تبلیغ، می‌تواند پیشرفت کند.

عنوان: The future of Twitter: Four scenarios
نویسنده: Darrell M. West
مرکز مطالعاتی: Brookings
تاریخ انتشار: November 22, 2022

استفاده از مقامات ملی رقابت برای اجرای قانون بازارهای دیجیتال

قانون بازارهای دیجیتال اتحادیه اروپا (DMA) با هدف تنظیم برخی از اقدامات ضدرقابتی غول‌های فناوری در ۱۴ سپتامبر ۲۰۲۲ به تصویب نهایی رسیده، از اول نوامبر ۲۰۲۲ لازم‌الاجرا شده و از ۶ ماه بعد یعنی از می ۲۰۲۳ قابل پیگرد خواهد بود. کمیسیون اروپا به‌عنوان تنها مجری این قانون، به‌علت محدودیت بودجه و منابع انسانی هنوز آمادگی اجرای آن را در سطح ۱۳ پلتفرم آنلاین فراگیر ذیل DMA ندارد. این اتفاق در عمل باعث شده است تا همان انتقاداتی که به اجرای قوانین ضدانحصار وارد بود و در پی آن قانون DMA تصویب شد، بر این قانون هم وارد بوده و اجرای آن را کم‌اثر کند.

یک راه‌حل می‌تواند این باشد که کمیسیون برای کمک به اجرای DMA به کشورهای اتحادیه اروپا مراجعه کرده و از ظرفیت آن‌ها استفاده کند. بااین‌حال، مقامات ملی رقابت (NCAs) در کشورهای اتحادیه اروپا درحال‌حاضر فاقد انگیزه برای مشارکت هستند. NCAها قبلاً چندین پرونده ضدانحصار را در بخش دیجیتال پیگیری و تکمیل کرده‌اند. بنابراین، کمیسیون باید با ارائه مشوق‌هایی برای کمک به اجرای DMA، بر تخصص آن‌ها تکیه کند.



عنوان	With a little help from some friends coordinating Digital Markets Act enforcement
نویسنده	Christophe Carugati
مرکز مطالعاتی	bruegel
تاریخ انتشار	November 10, 2022

سیاست ارتقای پهنای باند

ترویج فراگیر پهنای باند ثابت و سیار با کیفیت بالا و قیمتی مقرون‌به‌صرفه، عامل مهمی برای تحول دیجیتال جامعه بوده و به رفع شکاف دیجیتال کمک خواهد کرد. این موضوع در طول همه‌گیری کرونا که دسترسی به پهنای باند عامل مهمی برای کار، آموزش و پزشکی ازراه‌دور و تجارت الکترونیک بود، واضح‌تر شد.

ارائه دسترسی پهنای باند برای همه با قیمت مقرون‌به‌صرفه همیشه چالش‌برانگیز بوده است. همه‌گیری کرونا و حمله روسیه به اوکراین، منجر به گران‌تر شدن تقویت پهنای باند شد. افزایش رقابت، همراه با ارائه سریع و کارآمد دسترسی به منابعی مانند طیف الکترومغناطیسی و دسترسی به زمین و حق عبور و دیگر امکانات به بخش خصوصی، می‌تواند اهمیت ویژه‌ای در ارتقای آسان‌تر پهنای باند داشته باشد. برای مثال کشورهای G۲۰ اکنون به دنبال بهبود زیرساخت پایدار و عادلانه هستند؛ به این معنی که منابع جدید باید درآمدهای عمومی را برای توسعه پهنای باند اختصاص دهند. همچنین پهنای باند را می‌توان با استفاده از درآمدهای مالیاتی جدید مورد انتظار ناشی از اصلاحات مالیاتی جهانی که در سازمان همکاری اقتصادی و توسعه بر روی آن‌ها توافق شده است، تقویت کرد.

عنوان	Promotion of high capacity broadband to rebuild and recover from the pandemic
نویسنده	J. Scott Marcus , Alicia Garcia-Herrero , Lionel Guetta-Jeanrenaud
مرکز مطالعاتی	bruegel
تاریخ انتشار	November 23, 2022

گام‌های بعدی برای سیاست نیمه‌هادی ایالات متحده

سرمایه‌گذاری ۵۲٫۷ میلیارد دلاری «قانون تراشه» برای تولید نیمه‌هادی‌های داخلی با انگیزه تحقق سه هدف اصلی انجام می‌شود:

۱) کاهش احتمال اینکه شوک‌های خارجی عرضه تراشه‌ها را مختل کند، ۲) تقویت رقابت اقتصادی بین‌المللی آمریکا و ایجاد مشاغل داخلی و ۳) از نیمه‌هادی‌ها در برابر خرابکاری در فرآیند تولید محافظت شود.

این گزارش استدلال می‌کند که «قانون تراشه» به‌خودی‌خود هیچ‌یک از این اهداف را به‌طور کامل محقق نخواهد کرد. این اقدام یک گام بزرگ رو به جلو است، اما شکاف‌های متعددی در محورهای زیر بر جای می‌گذارد که نیازمند اقدامات بیشتر دولت است:

۱. سیاست‌گذاران باید اطمینان حاصل کنند که یارانه‌های ۳۹ میلیارد دلاری در قانون تراشه به‌طور مفید بین ساخت و مونتاژ، آزمایش و بسته‌بندی تقسیم می‌شود.
۲. دولت و صنعت باید با یکدیگر همکاری کنند تا آگاهی از نقاط کم‌توجه در زنجیره تأمین را بهبود بخشند؛ به‌ویژه آن‌هایی که ناشی از فعالیت‌های مدیریت زنجیره تأمین غیرشفاف به رهبری بخش خصوصی است.
۳. کاخ سفید و وزارت بازرگانی باید با کمک دانشمندان برجسته این مسئله را بررسی کنند که چگونه سیاست‌ها و ابتکارات اقتصادی می‌تواند فرصتی برای بخش‌هایی از نیروی کار داخلی ایجاد کند.
۴. دفتر برنامه تراشه «CHIPS» وزارت بازرگانی باید اطمینان حاصل کند که بودجه تحقیق‌وتوسعه از طرح‌هایی حمایت می‌کند که شرکت‌های آمریکایی را برای تغییرات پارادایم در فناوری نیمه‌هادی‌ها آماده می‌کند.
۵. مؤسسه ملی استاندارد و فناوری باید فرایندهای توسعه استانداردهای امنیتی نیمه‌هادی منبع‌باز را بین تولیدکنندگان و مصرف‌کنندگان عمده بین‌المللی نیمه‌هادی‌ها تسهیل کند.

عنوان	After the CHIPS Act: The Limits of Reshoring and Next Steps for U.S. Semiconductor Policy
نویسنده	vishnu Kannan, jacob feldgoise
مرکز مطالعاتی	Carnegie
تاریخ انتشار	November 22, 2022

مرور رویه قطع کردن اینترنت در آفریقا

اندیشکده کارنگی در نوامبر ۲۰۲۲ طی یادداشتی به مسئله خاموشی اینترنت در قاره آفریقا پرداخته است. نویسنده این یادداشت به طرح پرسش‌هایی در این زمینه پرداخته و پاسخ‌هایی برای آن ارائه می‌کند:

«قطع کردن اینترنت یک روش افراطی و درعین‌حال تکراری برای کنترل ارتباطات آنلاین است. در قاره آفریقا، اعم از دولت‌های خودکامه یا دموکراتیک، در واکنش به ترویج خشونت از طریق سخنان نفرت‌انگیز آنلاین یا اطلاعات نادرست در ایام انتخابات، معمولاً به قطع اینترنت متوسل شده‌اند. اما علاوه‌براین، حتی در زمانی که هیچ تهدیدی از جمله تظاهرات مسالمت‌آمیز نیز وجود نداشته، شاهد اختلالات جزئی یا سراسری شبکه اینترنت هستیم.»

«از دیدگاه شهروندان و کاربران که از فرصت‌های بهره‌گیری از داده‌های موجود در اینترنت محروم می‌شوند، قطع‌شدن اینترنت نامناسب و توهین‌آمیز به نظر می‌رسد. این اتفاق معمولاً ازسوی رهبرانی که مدت زیادی در سمت خود باقی مانده‌اند، مشاهده می‌شود؛ مانند پل بیا «Paul Biya» یا یووری موسوینی «Yoweri Museveni» از اوگاندا. آن‌ها خود را در اقدامات سرکوب‌گرانه برای تضمین انتخابات مسالمت‌آمیز یا جلوگیری از تهدید مداخله خارجی محق می‌دانند؛ اما آیا همه ادعاهای آن‌ها غیرقانونی است؟ آیا این اقدامات برای حفظ قدرت است؟ اگر این استدلال‌ها نه ازسوی آن‌ها، بلکه از منابع معتبرتر بود، چه نتیجه‌ای دربرداشت؟ در این یادداشت به این سؤالات و برخی دیگر از سؤالات پرداخته خواهد شد.»

عنوان	It's Time to Revisit the Framing of Internet Shutdowns in Africa
نویسنده	Iginio Gagliardone, Nicole Stremlau
مرکز مطالعاتی	Carnegie
تاریخ انتشار	November 21, 2022

سیاست جدید وزارت دفاع آمریکا برای استفاده از دستگاه‌های شخصی در محل کار

برنامه آزمایشی اخیر ارتش ایالات‌متحده که حمل دستگاه شخصی به محل کار (Bring Your Own Device یا BYOD) نامیده می‌شود؛ با ادغام فناوری در عصر اطلاعات و آینده‌نگری، استاندارد جدیدی را برای وزارت دفاع (DOD) تعریف و ایجاد می‌کند. حالت قبلی BYOD این بود که به یک کارمند اجازه می‌داد تا از دستگاه شخصی خود برای اتصال فیزیکی به شبکه دولتی و استفاده از آن در کل محیط کار استفاده کند. چنین برداشتی مساوی با یک حادثه بزرگ امنیت سایبری است. این سیاستی نیست که توسط وزارت دفاع آمریکا قابل‌پذیرش باشد. وزارت دفاع باید BYOD را مورد بررسی مجدد قرار دهد، چراکه دستگاه شخصی را قادر می‌سازد تا دسترسی قابل‌اعتمادی به شبکه دولت برای انجام تجارت عادی، رسمی و درعین حال رعایت انطباق با امنیت سایبری داشته باشد. ابتدایی‌ترین نکته‌ای که در بازتعریف جدید باید مورد توجه قرار گیرد، عدم ذخیره داده‌های دولتی در دستگاه‌های شخصی است.

منظور BYOD چیست و چرا بد است؟

اتصال مستقیم دستگاه شخصی کارمندان به شبکه دولتی یک حادثه امنیت سایبری ایجاد می‌کند، زیرا دستگاه‌های شخصی مشمول دستورالعمل‌های امنیتی سایبری سخت‌گیرانه وزارت دفاع آمریکا نیستند. اکثر اعضای سرویس هرگز نمی‌خواهند کنترل و نظارت کامل دستگاه شخصی خود را به‌منظور دسترسی به ایمیل کاری یا دسترسی به فایل مربوط به کار، به دولت واگذار کنند. بااین‌حال، تعریف کنونی وزارت دفاع از BYOD ایجاب می‌کند که دولت، یا کنترل کامل دستگاه‌های کاری را در دست بگیرد یا رضایت کاربر برای نظارت بر دستگاه کاری به‌منظور انجام امور رسمی را اخذ کند. به‌علاوه، BYOD با خرید، کارکرد و نگهداری دستگاه کاری کاربر، صرفه‌جویی زیادی در هزینه‌ها برای دولت به‌وجود می‌آورد. این دیدگاه یک اشتباه محاسباتی است زیرا اکثر اعضای سرویس به دولت اجازه نمی‌دهند که کنترل کامل یا رضایت خود را برای نظارت بر دستگاه شخصی خود در دست بگیرد.

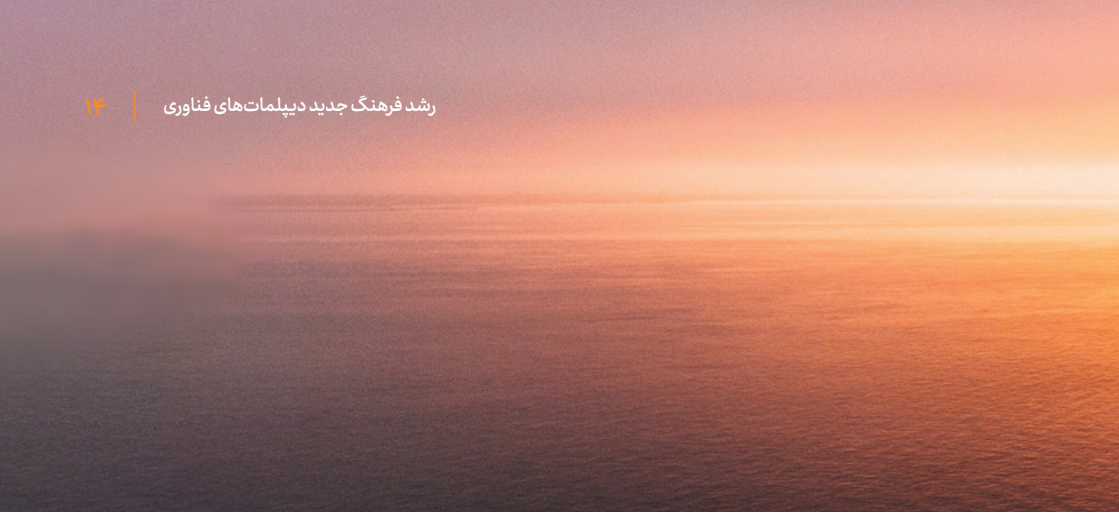
عنوان: Redefining DOD's Bring Your Own Device Policy
نویسنده: Atiim O. Phillips
مرکز مطالعاتی: CSIS
تاریخ انتشار: November 22, 2022

بهبود اجرای کنترل‌های صادراتی با استفاده از علم داده و هوش مصنوعی

از آن‌جایی که سیاست‌های فناوری آمریکا به‌طور فزاینده‌ای بر روی رقابت استراتژیک با روسیه و چین تمرکز دارد، کنترل صادرات در زمینه مسائل فناوری، به خط مقدم سیاست خارجی ایالات‌متحده تبدیل شده است. همان‌طور که مقامات دولت ایالات‌متحده بارها اعلام کرده‌اند؛ محدود کردن دسترسی روسیه به فناوری پیشرفته ازطریق کنترل‌های صادراتی، بخش مهمی از پاسخ ایالات‌متحده به تهاجم روسیه به اوکراین است.

متأسفانه، تقریباً تمام بحث‌ها بر این مبناست که آیا و چه زمانی باید کنترل‌های صادراتی اعمال شود. درحالی‌که باید بر چگونگی حصول اطمینان از اجرای مؤثر کنترل‌های صادراتی پس از اعمال، تمرکز کرد. دفتر صنعت و امنیت (BIS) در وزارت بازرگانی بر بیشتر کنترل‌های صادرات نظارت می‌کند. BIS با شبکه‌های فرار قاچاق و کنترل صادرات در سراسر جهان، به‌ویژه شبکه‌های تحت حمایت روسیه و چین، مقابله می‌کند. در این نشست آلن استیوز «Alan Estevez» درمورد بهبود سیاست‌ها در این زمینه با استفاده از هوش مصنوعی به گفتگو می‌پردازد. این گفتگو در ارتباط با گزارشی به قلم اوست.

عنوان	Improving Export Controls Enforcement Using Data Science and Artificial Intelligence
نویسنده	Gregory C. Allen, William Alan Reinsch
مرکز مطالعاتی	CSIS
تاریخ انتشار	September 6, 2022



مقررات‌گذاری فناوری می‌تواند به امنیت ملی آسیب برساند

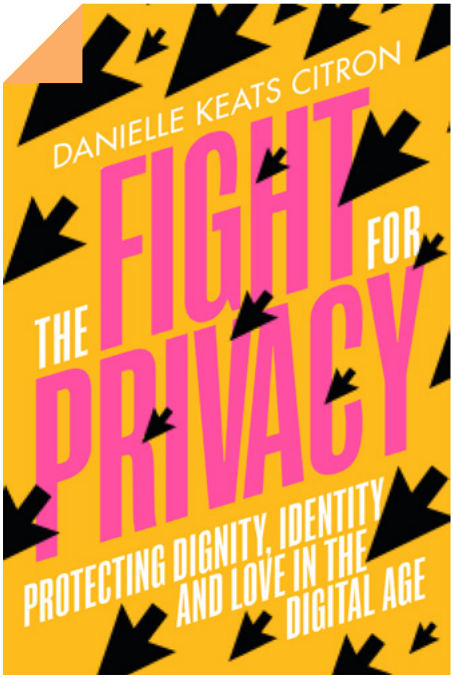
کمبود منابع مالی، تأمین امنیت دفاعی را سخت می‌کند. کشورهای اروپایی پس از دهه‌ها رشد آهسته، در مواجهه با تجاوز روسیه به اوکراین به این موضوع پی برده‌اند. ایالات‌متحده به لطف رشد اقتصادی خود، منابع موردنیاز برای امنیت ملی را در اختیار دارد، اما قوانین ضدانحصار پیشنهاد شده می‌تواند این وضعیت را تغییر دهد.

امنیت ملی به چیزی بیش از توانایی در به‌کارگیری سلاح‌های پیشرفته یا نیروهای بزرگ بستگی دارد و یکی از پایه‌های آن، مبتنی بر قدرت اقتصادی است که می‌تواند باعث ایجاد نفوذ و قدرت بین‌المللی شود. اکنون قدرت اقتصادی نیازمند یک بخش فناوری قوی است. این نتیجه‌گیری ممکن است برای برخی ناخوشایند باشد، اما باید باور داشت که ضعف بخش فناوری و شرکت‌های ضعیف این حوزه، غیرقابل قبول است.

هیچ‌کس ادعا نمی‌کند که غول‌های فناوری نباید تنظیم شوند، رفتارهای ناپسندی در جمع‌آوری داده‌های شخصی و ترجیح‌دادن خود ازسوی آن‌ها وجود دارد که باید تغییر کند. اما هیچ مقرراتی نباید به‌گونه‌ای وضع شود که نوآوری ایالات‌متحده را از بین ببرد.

عنوان	Tech Regulation Can Harm National Security
نویسنده	James Andrew Lewis
مرکز مطالعاتی	CSIS
تاریخ انتشار	November 28, 2022

رویداد کتاب مبارزه برای حفظ حریم خصوصی



در کتاب مبارزه برای حفظ حریم خصوصی، دنیل سیترون «Danielle Citron» توضیح می‌دهد که چگونه حریم خصوصی برای زندگی‌های صمیمی در معرض تهدید است. دیپ‌فیک‌ها، ایمیل‌های فاش‌شده و سوابق تلفن، رایانه‌های هک‌شده، و ترور ژورنالیستی شخصیت‌ها به‌آسانی قابل استفاده هستند و می‌توانند به خانواده، زندگی خصوصی، شهرت و شغل افراد آسیب‌های پایدار وارد کنند. اخیراً دستور لغو حق حریم خصوصی زنان و دختران در تصمیمات مربوط به باروری توسط دادگاه عالی به این معنی است که جستجوهای آنلاین و استفاده از اپلیکیشن و داده‌های مکان، نه‌تنها در تصمیم‌گیری‌های مربوط به بیمه کار و زندگی، بلکه در تحقیقات جنایی نیز مورد استفاده قرار خواهند گرفت. سیترون با مثال‌های واضحی که از مصاحبه با قربانیان، فعالان و قانون‌گذاران از سراسر جهان به دست آمده است، خواهان بازبینی حریم خصوصی به‌عنوان یک حق اساسی انسانی و مدنی شده و نقشه راهی برای درک و دفاع از حریم خصوصی در قرن بیست‌ویکم ارائه می‌دهد.

در این رویداد، سیترون با کیتلین چین «Caitlin Chin» نویسنده این کتاب درباره نحوه شکست سیستم حقوقی ایالات‌متحده در جلوگیری از جمع‌آوری و اشتراک‌گذاری داده‌های مضر و در نتیجه سوءاستفاده‌های محسوس از حریم خصوصی دیجیتال در سراسر جهان، صحبت می‌کند.

عنوان	Book Event: The Fight for Privacy with Danielle Citron
نویسنده	Danielle Citron
مرکز مطالعاتی	CSIS
تاریخ انتشار	December 5, 2022

همکاری مشترک برای حفظ فضای سایبری باز

چین قصد دارد فناوری اطلاعات را برای تبدیل شدن به ابرقدرت دیجیتال قرن بیست‌ویکم به یک ابزار اصلی تبدیل کند. اما چین تنها تهدید در فضای سایبری نبوده و تعداد بالای سارقان اطلاعات در حوزه سایبری یک چالش مهم به‌شمار می‌آید. برای تضمین آینده‌ای صلح‌آمیز و پیشرفته، باید ضمن تمرکز بر اشتراکات سایبری و همکاری‌های چندجانبه، جهان اطلاعات را آزاد و باز نگه داریم.

این مأموریت باید در سه جنبه انجام شود: الف) حفظ فضای باز برای تبادل آزاد ایده‌ها، بحث، همکاری و به اشتراک‌گذاری اطلاعات، ب) ایجاد یک محیط امن، محافظت‌شده از فعالیت‌های مخرب و غیرقانونی و ج) حفظ فضای مجازی باز درجهت دسترسی آزاد و محیطی برای کسب‌وکار و تولید ثروت. هیچ‌یک از این‌ها به‌تنهایی وظایف دولت نیست و همچنین نباید مردم فقط بر اساس منافع شرکت‌ها اداره شوند. جامعه مدنی نقش مهمی در پیوند صداهای برآمده، خلاق، معتبر و دانش فنی دارد که متعهد به پیشبرد آزادی، امنیت و رفاه برای همه هستند.

ابتکارات جدیدی برای تحقق این موارد مورد نیاز است. در این یادداشت، چارچوب لازم برای مطابقت با چالش‌ها و فرصت‌های دنیای آزاد امروز در فضای سایبری، بیان می‌شود.

عنوان	Protecting the Cyber Commons: A Band of Brothers Approach
نویسنده	Kiron K. Skinner, Ph.D., Dustin Carmack, James Jay Carafano
مرکز مطالعاتی	CSIS
تاریخ انتشار	November 21, 2022

فناوری 5G در صنعت دفاعی آمریکا

بلوغ آهسته شبکه‌های تجاری 5G در ایالات‌متحده می‌تواند برای وزارت دفاع ایالات‌متحده (DoD)، که توانایی تطبیق فناوری‌های مرتبط با 5G را دارد، ناامیدکننده باشد. وزارت دفاع با معکوس کردن نقش سنتی خود به‌عنوان توسعه‌دهنده فناوری جدید و در عوض تبدیل شدن به یک مشتری، می‌تواند بهتر از پتانسیل 5G استفاده کند و از سرمایه‌گذاری تریلیون دلاری بخش خصوصی در اتصال تلفن همراه استفاده کند.

این مطالعه بررسی می‌کند که وزارت دفاع چگونه می‌تواند سخت‌افزار و نرم‌افزار تجاری 5G را برای سیستم‌های طیف الکترومغناطیسی (EMS) آینده جمع‌آوری نماید. عدم انجام این کار خطراتی را به همراه خواهد داشت، زیرا دشمنان می‌توانند همین فناوری‌ها را به دست آورده، جمع‌آوری کرده و به کار گیرند. بهره‌برداری از پیشرفت‌های تجاری 5G می‌تواند الگویی باشد برای اینکه ارتش ایالات‌متحده دریابد که چگونه باید الزامات و فرآیندهای تحقیق‌وتوسعه خود را بازبینی کند تا نقش رو به کاهش دولت در بسیاری از زمینه‌های نوآوری را منعکس نموده و همچنین تغییر نقش این دستگاه از توسعه‌دهنده به مشتری را بازنمایی کند.

عنوان	Exploiting the Fast-Follower Advantage: Making 5G the Ultimate Parts Bin and Adopting a Commercial-First Approach to Military Acquisition
نویسنده	Bryan Clark , Dan Patt
مرکز مطالعاتی	Hudson
تاریخ انتشار	November 23, 2022

سیاست‌های جلوگیری از انتشار اظهارنظرهای جعلی آنلاین

برخی از کسب‌وکارها، برای جذب مشتری و یا دستکاری شهرت خود یا رقبایشان، به ارسال آنلاین نظرات جعلی روی می‌آورند. این اظهارنظرهای جعلی مشتریان را فریب می‌دهد تا کالاها یا خدماتی با کیفیت ناشناخته یا نامرغوب را خریداری کنند؛ لذا این دستکاری‌ها به اعتبار کسب‌وکارهای صادق آسیب رسانده و میلیاردها نفر را در تجارت الکترونیک تحت تأثیر قرار می‌دهد. متأسفانه، درحالی‌که صنعت و دولت گام‌های مهمی برای مقابله با گسترش آن‌ها برداشته‌اند، شیوع بررسی‌های جعلی احتمالاً در کنار اقتصاد دیجیتال رشد کرده است.

در این نشست که در مرکز نوآوری داده‌ها «ITIF» برگزار شده درمورد شیوع بررسی‌های آنلاین جعلی، تأثیر آن‌ها بر شرکت‌ها و مصرف‌کنندگان و اقداماتی که سیاست‌گذاران می‌توانند برای جلوگیری از گسترش آن‌ها انجام دهند، بحث شده است.

عنوان	How Can Policymakers Deter Fake Online Reviews?
نویسنده	Becca Trate
مرکز مطالعاتی	ITIF
تاریخ انتشار	January 19, 2023

چشم‌انداز سیاست هوش مصنوعی ایالات‌متحده

گفتمان سیاست درمورد هوش مصنوعی در ایالات‌متحده در بالاترین سطح خود قرار دارد. صدوهفدهمین جلسه کنگره، متمرکزترین جلسه ادوار با موضوع هوش مصنوعی بود. در صدوهجدهمین جلسه کنگره که در ژانویه تشکیل می‌شود، احتمالاً روند صعودی پرداختن به هوش مصنوعی ادامه پیدا خواهد کرد. به همین دلیل اکنون، زمان بسیار مهمی است تا دستاوردهای سیاست هوش مصنوعی ایالات‌متحده تا به امروز و همچنین زمینه‌هایی که برای پیشرفت مداوم ایالات‌متحده وجود دارد، مورد بررسی قرار گیرد.

در مرکز نوآوری داده‌ها «ITIF» یک میزگرد درمورد اثربخشی سیاست هوش مصنوعی تا به امروز برگزار شده است؛ کارشناسان درمورد اینکه چگونه سیاست‌گذاران می‌توانند به بهترین وجه توانایی‌ها و فعالیت‌های اکوسیستم هوش مصنوعی ایالات‌متحده را در حرکت رو به جلو پرورش دهند، بحث می‌کنند.

عنوان	Where Should US AI Policy Be Headed Next?
نویسنده	Hodan Omaar
مرکز مطالعاتی	ITIF
تاریخ انتشار	January 17, 2023

اقتصاد فناوری هند

معمولاً هر فردی اگر حداقل یکبار از فین‌تک‌ها استفاده نکرده باشد، حتماً درباره آن شنیده است. حتی اگر یک مصرف‌کننده فین‌تک نباشد، ممکن است درمورد رشد، چالش‌های آن، مشارکت مصرف‌کننده و همچنین سوءاستفاده احتمالی آن‌ها شنیده باشد.

آنچه مهم است، توجه به تفاوت اقتصاد فناوری «TechFins» با فناوری اقتصادی «FinTechs» است. اقتصاد فناوری با فناوری اقتصادی از نظر نحوه ایجاد کسب‌وکار، مدل‌های کسب‌وکار، درآمدزایی، قابلیت‌های فناوری، و توانایی افزایش سرمایه سهام و پیشنهادات اصلی مصرف‌کننده متفاوت هستند. اقتصاد فناوری با استفاده از شبکه‌ها، فناوری و دسترسی مصرف‌کننده به پلتفرم، مقادیر عظیمی از داده‌ها را درباره مصرف‌کنندگان جمع‌آوری می‌کند که معمولاً از یک رابطه غیرمالی جمع‌آوری می‌شوند. اقتصاد فناوری منابع و توانایی تجزیه‌وتحلیل داده‌ها را در به‌صورت لحظه‌ای برای ارائه خدمات مالی دارند. از نظر تئوری، آن‌ها حتی می‌توانند پیشنهاداتی ارائه کنند که برای هر مصرف‌کننده‌ای جذاب باشد. نمونه‌های محبوب جهانی اقتصاد فناوری عبارتند از Google، Facebook، Baidu، Apple، Amazon، Alibaba و Tencent، در این مقاله به بررسی زمینه‌های حضور کاربران در این فضا و رفتار تنظیم‌گرها در این رابطه پرداخته است.

عنوان	Indian TechFin: Are regulations sufficient enough?
نویسنده	Srinath Sridharan
مرکز مطالعاتی	ORFonline
تاریخ انتشار	November 28, 2022

توافق چهارجانبه پیرامون امنیت سایبری

کشورهای مختلف در منطقه هند و اقیانوس آرام شاهد افزایش تعداد و شدت تهدیدات امنیت سایبری خود هستند. چالش‌های نوظهور شامل تهدیدات امنیت ملی و آسیب‌پذیری‌های زنجیره تأمین بین‌المللی و همچنین سلاح‌سازی فضای سایبری توسط بازیگران دولتی و غیردولتی است. در پاسخ به این چالش‌ها، گفتگوی چهارجانبه امنیتی (متشکل از هند، استرالیا، ژاپن و ایالات‌متحده) «Quad» به‌عنوان یک رهبر کلیدی در شکل دادن به هنجارها و صف‌بندی‌های امنیتی در حال ظهور است. به شکل یک قالب جدید چندجانبه در منطقه، همکاری این چهار کشور برای مقابله با چالش‌های بین‌المللی روبه‌رشد در اقیانوس هند و اقیانوس آرام، به‌ویژه چالش‌های مربوط به ظهور چین به‌عنوان یک قدرت بزرگ، آغاز شد.

تلاش فزاینده Quad برای شکل دادن به هنجارها و قوانین بین‌المللی در هند و اقیانوس آرام در محیطی مملو از چالش‌های متعدد صورت می‌گیرد. رشد قاطعانه چین و همچنین اختلافات داخلی در این گروه، خطرات قابل‌توجهی را برای مأموریت ایجاد یک پلتفرم چندجانبه جهت رسیدن به یک هند و اقیانوس آرام آزاد، باز و امن ایجاد می‌کند. با تمرکز بر همکاری امنیت سایبری Quad، این گزارش به بررسی خطرات داخلی و خارجی مختلفی می‌پردازد که کشورهای Quad درحال‌حاضر در مشارکت خود با آن‌ها مواجه هستند.

عنوان	Quad Vadis? A Risk Assessment of the Quad's Emerging Cybersecurity Partnership
نویسنده	Tobias Scholz
مرکز مطالعاتی	ORFonline
تاریخ انتشار	November 30, 2022

آیا آمریکا از امنیت سایبری چشم‌پوشی کرده است؟

در این گفتگو با رابرت اوبراین«Robert O'Brien»، مشاور سابق امنیت ملی آمریکا درمورد پیامدهای امنیت سایبری مصاحبه شده است. اوبراین بیشتر وقت خود را صرف بررسی جایگاه ایالات‌متحده در رقابت فناوری کرده و اینکه چگونه دشمنان آمریکا از فناوری با نگاه امنیت ملی، ازجمله ترویج اقتدارگرایی دیجیتال، استفاده می‌کنند. او در چندین سمت دیپلماتیک ازجمله فرستاده ویژه ریاست جمهوری در امور گروگان‌ها در وزارت امور خارجه و در آخرین خدمت خود به‌عنوان بیست‌وهفتمین مشاور امنیت ملی رئیس‌جمهور، حضور داشته است. در این نشست رابرت اوبراین به سؤالات زیر پاسخ داده است:

۱. چگونه تکامل فناوری در طول زمان بر امنیت ملی تأثیر می‌گذارد؟
۲. آیا قانون تراشه به تأمین امنیت سایبری کمک می‌کند؟
۳. وضع قوانین در این حوزه چه کمکی به حکمرانی فناوری می‌کند؟

عنوان	Have We Turned a Blind Eye to Cybersecurity? Highlights from My Conversation with Ambassador Robert O'Brien
نویسنده	Robert O'Brien
مرکز مطالعاتی	AEI
تاریخ انتشار	December 1, 2022

سرمایه‌گذاری در وب۳

لورن استفانیان «Lauren Stephanian» و براندون هافمن «Brandon Hoffman» در نشست سرمایه‌گذاری در وب۳ به گفتگو پرداخته و با توصیف نفوذ فناوری‌های وب ۳ به حوزه‌های گوناگون صنعت، به بررسی دیدگاه‌های سرمایه‌گذاران در زمینه‌هایی نظیر زیرساخت، ابزارهای توسعه‌دهنده و حوزه‌های نوآورانه مانند NFT پرداختند.

سقوط Terra/Luna، FTX و اثر دومینویی آن در سراسر اکوسیستم منجر به ایجاد فضای محافظه‌کارانه‌تر برای جمع‌آوری سرمایه در حوزه استارت‌آپ‌های وب۳ و درس‌های زیادی برای سرمایه‌گذاران شده است. بااین‌حال، این رویدادها می‌توانند توسعه مقررات شفاف‌تر را تسریع کرده و شفافیت بیشتری را برای سازندگان در این فضا به ارمغان بیاورد.

عنوان	Event Recap: Investing in Web3
نویسنده	Lauren Stephanian, Brandon Hoffman
مرکز مطالعاتی	Belfercenter
تاریخ انتشار	December 1, 2022

DMA و ممنوعیت خودترجیحی پلتفرم‌های دیجیتال

پلتفرم‌های آنلاین پرکاربر واسطه بین کاربران نهایی و کاربران تجاری هستند. آن‌ها گاهی اوقات محصولات و خدمات خود را در کنار محصولات رقبا پیشنهاد می‌کنند. این می‌تواند منجر به تبعیض توسط پلتفرم‌هایی شود که پیشنهادات خود را با اولویت بالاتری نسبت به رقبا ارائه می‌دهند.

قانون بازارهای دیجیتال اتحادیه اروپا (DMA)، پلتفرم‌های آنلاین بزرگ را از برخورد تبعیض‌آمیز نسبت به محصولات و خدمات رقبا هنگام رتبه‌بندی، خزیدن و نمایه‌سازی منع می‌کند. پلتفرم‌ها یا Gatekeeperها در تعریف DMA - باید شرایط شفاف، منصفانه و بدون تبعیض را هنگام رتبه‌بندی محصولات و خدمات اعمال کنند. بااین‌حال، شناسایی، تشخیص، انطباق و نظارت بر خودترجیحی پیچیده و نیازمند منابع است و این کار به رویکرد مورد به مورد و دسترسی و تجزیه‌وتحلیل داده‌ها و الگوریتم‌های پلتفرم نیازمند است.

DMA به دروازه‌بانان اجازه می‌دهد تا محصولات و خدمات خود را در شرایط مساوی با رقبا تبلیغ کنند. با وجود این، DMA رفتار مساوی و عناصر اصلی خودترجیحی را تعریف نمی‌کند.

برای سهولت اجرا، کمیسیون اروپا باید دستورالعملی را درمورد آنچه که بر اساس DMA به‌منزله خودترجیحی است، صادر کرده و دو اصل اصلی را مشخص کند. اول، دروازه‌بانان باید از پارامترهای عینی و بی‌طرفانه برای تعیین رتبه‌بندی، نمایه‌سازی و خزیدن استفاده کنند. دوم اینکه دروازه‌بانان باید رفتار مساوی و عادلانه از خود نشان دهند.

راهنمایی، انطباق را آسان‌تر می‌کند. لذا کمیسیون باید در مرحله بعد با انتصاب و اطمینان از چرخش کافی حساب‌رسان خارجی برای جلوگیری از خودترجیحی توسط دروازه‌بانان، بر رعایت آن نظارت کند. کمیسیون همچنین باید با همکاری مقامات ذی‌صلاح ملی که ابزارهای فناورانه را توسعه می‌دهند، بر عدم‌انطباق‌ها نظارت کرده و مصادیق ممنوعیت خودترجیحی را به‌صورت موردی مشخص کند.

عنوان	How to implement the self-preferencing ban in the European Union's Digital Markets Act
نویسنده	Christophe Carugati
مرکز مطالعاتی	Bruegel
تاریخ انتشار	December 2, 2022

مقدمه‌ای بر ائتلاف آزادی آنلاین

سیاست‌گذاران خواستار «اتحادهای فناوری دموکراتیک» در همه‌چیز از زنجیره تأمین گرفته تا فناوری نوظهور و آزادی جهانی اینترنت هستند. این امر توجه به ائتلاف آزادی آنلاین (Freedom Online Coalition یا FOC) را که شامل سی‌وپنج کشور عضو متعهد به پیشبرد آزادی اینترنت و حقوق بشر آنلاین می‌باشد، جلب کرده است. مأموریت FOC اکنون بیش از هر زمان دیگری در تاریخ یازده‌ساله خود فرصت‌هایی را برای کشورهای عضو فراهم می‌کند تا اقدامات زیر را انجام دهند:

۱. هماهنگی اقدامات دیپلماتیک عمومی و خصوصی در پاسخ به تهدیدات علیه دموکراسی و حقوق بشر آنلاین؛
۲. همکاری در انجمن‌های چندجانبه برای تقویت هنجارها و استانداردهای همسو با حقوق بشر برای اکوسیستم دیجیتال؛
۳. ایجاد یک فضای قابل‌اعتماد برای همکاری با جامعه مدنی و بازیگران صنعت که به‌عنوان مرکز ثقل برای اقدامات استراتژیک مشترک عمل کند.

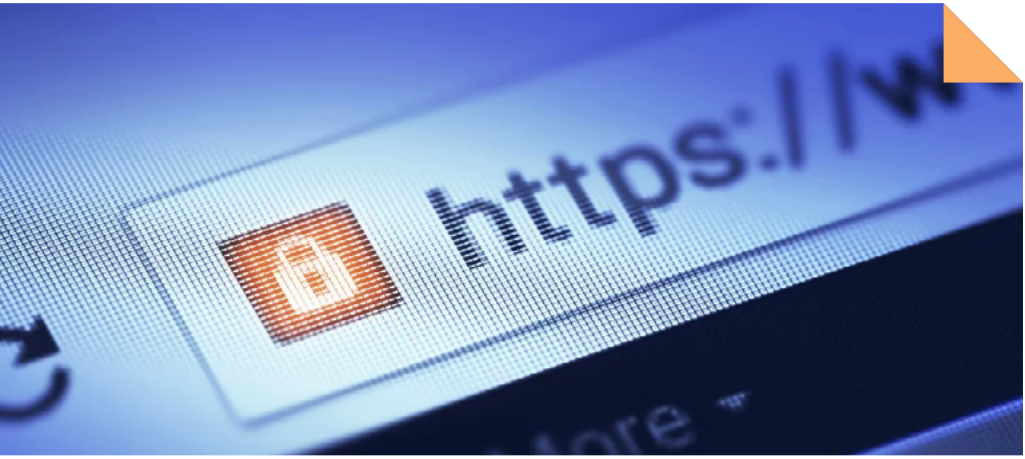
درعین‌حال، FOC به‌عنوان یک نهاد در نقطه عطف قرار دارد. از آن‌جایی که دموکراسی‌ها به دنبال مکانیسم‌هایی برای پیشبرد همکاری و اقدام در فضای جهانی متخاصم هستند، کشورهای عضو FOC فرصتی برای تقویت، شفاف‌سازی و تمرکز انرژی ازطریق ائتلاف دارند. این کار مستلزم آن است که اعضا به بحث‌های طولانی‌مدت مربوط به حوزه کاری، مشوق‌ها و تأثیر آن در مجامع بین‌المللی بپردازند.

عنوان: An introduction to the Freedom Online Coalition
نویسنده: Rose Jackson , Leah Fiddler, Jacqueline Malaret
مرکز مطالعاتی: Atlanticcouncil
تاریخ انتشار: December 6, 2022

استراتژی دفتر ملی سایبری

در این نشست کامیل استوارت گلاستر «Camille Stewart Gloster» معاون مدیر ملی سایبری ایالات‌متحده به گفتگو پیرامون محورهای زیر پرداخت:

۱. نقش و مسئولیت دفتر ملی سایبری و چگونگی ارتقای رهبری و ظرفیت فناوری ایالات‌متحده؛
۲. درس‌هایی پیرامون ویژگی‌های نیروی کار تخصصی حوزه سایبر؛
۳. نحوه تعامل دفتر ملی سایبری با بخش خصوصی و جامعه مدنی؛
۴. چگونگی افزایش مشارکت مردم در دفتر ملی سایبری؛
۵. روند کارآموزی در دفتر ملی سایبری، جذب نیرو از دبیرستان‌ها و نتایج آن؛
۶. تلاش‌هایی برای حفظ اینترنت رایگان، باز، ایمن و قابل همکاری.



عنوان	Camille Stewart breaks down the Office of the National Cyber Director's whole-of-society strategy
نویسنده	Camille Stewart Gloster
مرکز مطالعاتی	Atlanticcouncil
تاریخ انتشار	December 7, 2022

ارزیابی کارآمدی دفاع سایبری

تجربه واقعی جنگ سایبری در اوکراین بسیار متفاوت‌تر از پیش‌بینی‌ها بود؛ درحالی‌که روسیه از قابلیت‌های سایبری خود استفاده کرد، این حملات دیجیتالی بسیار کمتر از پیش‌بینی‌های ناظران در اوایل جنگ، موفقیت‌آمیز واقع شد.

چرا روسیه نتوانست در میدان نبرد دیجیتال پیروز شود؟ در اجلاسی که مقامات دولت اوکراین و ایالات‌متحده و شرکت‌های فناوری غربی که برای حمایت از دفاع دیجیتال اوکراین گرد هم آمده بودند، استدلال‌ها بر این استوار بود که شکست روسیه تا حدودی به دلیل پیچیدگی دفاعی «کی‌یف» است. اما ارزیابی این ادعا بسیار دشوار بوده و یک مشکل اساسی را برای سنجش وضعیت فعلی تحقیقات و سیاست امنیت سایبری نشان می‌دهد. همچنین، هیچ کتابی برای سنجش اثربخشی تلاش‌های دفاع سایبری یا انتقال دانش به مردم وجود ندارد و این امر نتیجه‌گیری از جنگ در اوکراین را برای اطلاع از وضعیت دفاعی آینده دشوار می‌کند. ارزیابی اثربخشی دفاع سایبری، بخش مهمی از توسعه سیاست امنیت سایبری و تصمیم‌گیری درباره مکان و نحوه سرمایه‌گذاری در شبکه‌ها و زیرساخت‌های رایانه‌ای است. اما در غیاب معیارهای دفاعی مطلوب، اندازه‌گیری این سرمایه‌گذاری‌ها دشوار است.

*

)

عنوان	How do we know when cyber defenses are working?
نویسنده	Josephine Wolff
مرکز مطالعاتی	Brookings
تاریخ انتشار	December 5, 2022

تنظیم‌گری ارزهای دیجیتال توسط دولت فدرال

افزایش علاقه به ارزهای رمزنگاری‌شده و رونق صرافی ارزهای دیجیتال FTX، این واقعیت را که دستگاه نظارتی امروزی برای نظارت بر این فناوری جدید مالی مجهز نیست، در کانون توجه قرار می‌دهد. کمیسیون بورس و اوراق بهادار، کمیسیون معاملات آتی کالا، شرکت بیمه سپرده فدرال، کنترل‌کننده ارز و فدرال رزرو همگی در حال مبارزه برای تحقق بهترین نحوه نظارت بر ارزهای دیجیتال هستند. چندین پیشنهاد در کنگره در دست بررسی است. یک استدلال این است که آسیب‌ها متوجه مصرف‌کنندگان بوده و ثبات مالی نیازمند قوانین جدید است. استدلال دیگر می‌گوید که تنظیم مقررات ارز دیجیتال به آن مشروعیت می‌بخشد لذا بهتر است آن را به حال خود رها کنیم.

در ۲۰ دسامبر، مرکز هاچینز (Hutchins Center) در سیاست‌های مالی و پولی و مرکز مقررات و بازارها میزبان مناظره مجازی درمورد این موضوع بود. پیتر کانتی-براون «Peter Conti-Brown» در جایگاه موافق تنظیم ارزهای دیجیتال و استفان سچتی «Stephen Cecchetti» از مدرسه بین‌المللی بازرگانی برندیس، در نقش مخالف، به بحث پرداختند.

عنوان	A debate: Should crypto be regulated by the federal government?
نویسنده	Peter Conti-Brown
مرکز مطالعاتی	Brookings
تاریخ انتشار	December 20, 2022

ژئوپلیتیک هوش مصنوعی و ظهور حاکمیت دیجیتال

پس از نشست ۲۹ سپتامبر ۲۰۲۱ شورای تجارت و فناوری ایالات‌متحده و اتحادیه اروپا؛ این دو مجموعه مخالفت خود را با حکمرانی هوش مصنوعی اعلام کردند، چراکه این حکمرانی به حقوق بشر ازجمله سیستم‌های امتیازدهی اجتماعی احترام نمی‌گذارد. در این جلسه، شورای تجارت و فناوری (Trade and Technology Council یا TTC) تصریح کرد که «ایالات‌متحده و اتحادیه اروپا نگرانی‌های قابل‌توجهی نسبت به عملکرد دولت‌های مستبد دارند، چراکه سیستم‌های امتیازدهی اجتماعی را با هدف اجرای کنترل اجتماعی در مقیاس آزمایشی اجرا می‌کنند. این سیستم‌ها آزادی‌های اساسی و حاکمیت قانون را تهدید می‌نمایند؛ برای مثال حکومت‌های مستبد این کار را ازطریق حذف سخنان مخالف حاکمیت، مجازات تجمعات مسالمت‌آمیز و سایر فعالیت‌های بیانی و تقویت سیستم‌های نظارت خودسرانه یا غیرقانونی انجام می‌دهند.»

این گزارش ابتدا مواضع منحصربه‌فرد اتحادیه اروپا، ایالات‌متحده و چین را درمورد تنظیم داده‌ها و حاکمیت هوش مصنوعی شرح داده و سپس پیامدهای رویکردهای مختلف برای جداسازی فناوری را مورد بحث قرار می‌دهد. در پایان نتایج سیاست‌های خاص پیرامون هوش مصنوعی، مانند قانون پاسخگویی الگوریتمی ایالات‌متحده، قانون هوش مصنوعی اتحادیه اروپا و مقررات چین درمورد موتورهای توصیه‌گر را بررسی می‌کند.

عنوان	The geopolitics of AI and the rise of digital sovereignty
نویسنده	Benjamin Cedric Larsen
مرکز مطالعاتی	Brookings
تاریخ انتشار	December 8, 2022

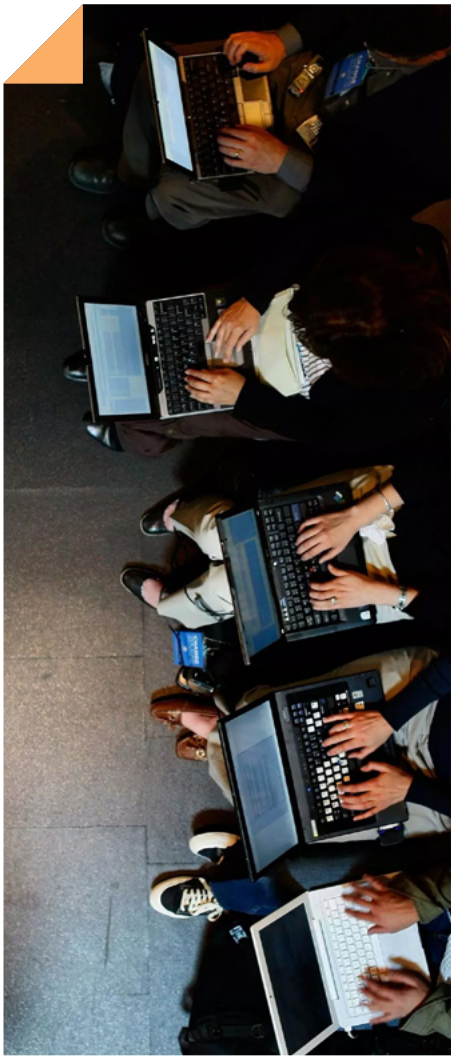
کمک قانون حفظ حریم خصوصی به تنظیم مقررات تبلیغات

در بحث بر سر قوانین فدرال مؤلفه‌های حفظ حریم خصوصی، تبلیغات و بازاریابی به چشم می‌خورد. شوشانا زوبوف، روان‌شناس اجتماعی، اصطلاح «سرمایه‌داری نظارتی» را برای توصیف مدل کسب‌وکار تبلیغاتی که بر پایه کسب درآمد از جمع‌آوری، استفاده و اشتراک‌گذاری اطلاعات دیجیتال ساخته شده، ابداع کرد و به کمیته مجلس توضیح داد که این مدل «بر این فرض استوار است که حریم خصوصی باید از میان برود». مبحث او توسط کمیسیون تجارت فدرال (FTC) در اعلامیه قوانین حفظ حریم خصوصی در آگوست گذشته برجسته شد که طی آن تحقیقات پیرامون «نظارت تجاری» را چارچوب‌بندی می‌کند.

تبلیغات دیجیتال عامل مهمی در گسترش نامحدود اطلاعات شخصی است. در وضعیت موجود، اکثر شرکت‌ها خود قوانین نحوه جمع‌آوری، استفاده و اشتراک‌گذاری داده‌های شخصی (سیستم‌های پیچیده‌ای که از تبلیغات دیجیتال پشتیبانی می‌کنند) را بدون هیچ‌گونه محدودیتی تعیین می‌کنند. قانون حفظ حریم خصوصی و حفاظت از داده‌های آمریکا (ADPPA)، لایحه‌ای که مجلس نمایندگان با ۵۳ رأی موافق در برابر ۲ رأی مخالف تصویب کرد، فراتر از هر لایحه جامع حریم خصوصی دیگری است که برای تعیین مرزهای عینی درخصوص جمع‌آوری، استفاده و اشتراک‌گذاری اطلاعات شخصی پیشنهاد یا تصویب شده است.

عنوان	Rulemaking in privacy legislation can help dial in ad regulation
نویسنده	Cameron F. Kerry , Mishaela Robison
مرکز مطالعاتی	Brookings
تاریخ انتشار	December 5, 2022

درس‌هایی از اقتصاد گیگ آنلاین



یکی از سریع‌ترین و مرتبط‌ترین بخش‌های بازار کار در سطح جهانی، اقتصاد گیگ آنلاین است که به ما درباره چگونگی توسعه بازارهای کار از راه دور می‌گوید. کار آنلاین یا «گیگ» (کار مبتنی بر پروژه) توسط یک بازار دیجیتال تسهیل می‌شود که ازطریق آن خدمات در سراسر جهان به‌وسیله پلتفرم‌هایی مانند Fiverr و Upwork صورت می‌گیرد.

در تئوری، این کار با واسطه آنلاین باید از منطق کم‌هزینه «برون‌سپاری» تبعیت کند، زیرا بازار کار آنلاین ذاتاً دیجیتالی است و تنظیم نشده است. بااین‌حال، ما ۱٫۸ میلیون گیگ ارائه‌شده در بیش از ۱۰۰ کشور بین سال‌های ۲۰۱۳ تا ۲۰۲۰ را بررسی کردیم و دریافتیم که کار حرفه‌ای از این منطق پیروی نمی‌کند. بسیاری از تقاضای کارهای حرفه‌ای آنلاین ازسوی مشتریانی در سواحل شرقی و غربی ایالات‌متحده برای نیروی کار در اروپای غربی و در استرالیا ارسال می‌شود، درحالی‌که بسیاری از کارگران آنلاین از اروپای شرقی، آسیای جنوبی و فیلیپین می‌آیند.

عنوان: The ‘anywhere’ jobs are not everywhere; they’re in cities
نویسنده: Fabian Stephany
مرکز مطالعاتی: Bruegel
تاریخ انتشار: December 7, 2022

کمیسیون اروپا باید براساس قانونِ بازارهای دیجیتال، کدام ادغام‌ها را بررسی کند؟

غول‌های فناوری بین سال‌های ۱۹۸۷ تا ژوئیه ۲۰۲۲، ۱۱۴۹ شرکت را در بخش‌های مختلف اقتصادی خریداری کردند. کمیسیون اروپا تنها ۲۱ مورد از این ادغام‌ها را بررسی کرد، درحالی‌که اکثر آن‌ها حدود کنترلی ادغام در اتحادیه اروپا را برآورده نمی‌کردند. این نشان‌دهنده اجرای ناقص قوانین است که با عدم نظارت بر ادغام‌های مسئله‌دار بازار رقابتی را به خطر انداخته است.

قانون بازارهای دیجیتال اتحادیه اروپا، که در نوامبر ۲۰۲۲ لازم‌الاجرا شد، تعهداتی را برای پلتفرم‌های خدمات پایه نظیر موتور جستجو که اصطلاحاً Gatekeeper نامیده می‌شوند، در نظر گرفته است. یکی از مهم‌ترین موارد این قانون لزوم اطلاع‌رسانی شرکت‌ها درمورد تمامی خریدها و ادغام‌های آتی خود در این حوزه است. این قانون باید بتواند گزارش‌های ارجاعی از سوی مقامات محلی را در این حوزه با استفاده از ظرفیت‌های کمیسیون با دقت ویژه مورد بررسی قرار دهد.

دستورالعمل فعلی کمیسیون اروپا درباره فرایند ارجاع و رسیدگی به پرونده‌های ادغام، انعطاف‌پذیر اما غیرعملی است، زیرا به‌جای معیارهای واضح و عینی، بر نظریه‌ها تکیه دارد. بدون شفاف‌سازی، ممکن است ادغام‌های بدون مشکل نیز در فرایند بررسی قرار گرفته و موجب تخصیص ناکارآمد منابع انسانی شود، اما عدم‌اطمینان قانونی همچنان ادامه داشته باشد. ازاین‌رو لازم است تا کمیسیون دستورالعمل جدیدی را مبنی بر احتمال مشکل‌ساز بودن ادغام‌های دیجیتالی صادر کند.

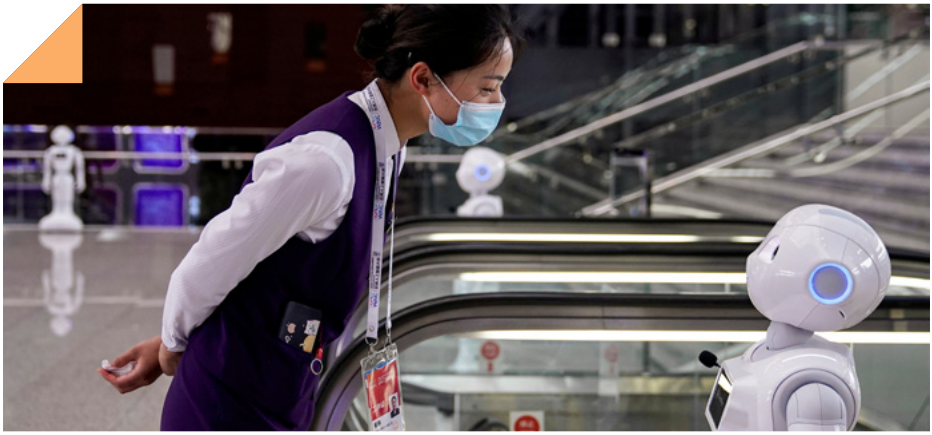
عنوان: Which mergers should the European Commission review under the Digital Markets Act?
نویسنده: Christophe Carugati
مرکز مطالعاتی: Bruegel
تاریخ انتشار: December 9, 2022

الگوریتم چین درباره حکمرانی هوش مصنوعی

دولت چین طی سال ۲۰۲۲ برخی آزمایش‌های ابتدایی را در زمینه ساخت ابزارهای نظارتی کنترل هوش مصنوعی انجام داده است. در این فرایند، چین در حال تلاش برای مقابله با مشکلی است که به‌زودی کلیه دولت‌ها با آن مواجه خواهند شد؛ اینکه آیا تنظیم‌گران می‌توانند بینش معناداری درمورد عملکرد الگوریتم‌ها به دست آورند و از عملکرد آن‌ها در محدوده‌های قابل‌قبول اطمینان حاصل کنند یا خیر.

سیستم ثبت‌نام اجباری الگوریتم‌های توصیه‌گری به دلیل تأثیراتش در چین و همچنین از نقطه‌نظر درس‌هایی که برای فناوران و سیاست‌گذاران در سایر کشورهای دارد، شایسته توجه است. اگرچه جزئیات کامل رجیستری این الگوریتم‌ها عمومی نشده است، اما با کندوکاو در کتابچه راهنمای دستورالعمل آنلاین آن، می‌توانیم بینش‌های جدیدی را در خصوص معماری نظارتی درحال‌ظهور چین برای الگوریتم‌ها آشکار کنیم.

تمرکز بر نقش الگوریتم‌های توصیه‌گری در انتشار اطلاعات، حفظ امنیت ملی و منافع عمومی، حدود آسیب‌رسانی به منافع مشروع کاربران، میزان رفتار انحصاری الگوریتم‌ها در پلتفرم‌های بزرگ و قابلیت‌های بسیج عمومی ازجمله مواردی است که در رویه جدید مورد توجه قرار گرفته است.



عنوان	What China's Algorithm Registry Reveals about AI Governance
نویسنده	Matt sheehan, Sharon du
مرکز مطالعاتی	Bruegel
تاریخ انتشار	December 9, 2022

تکه‌تکه‌شدن اینترنت؛ جدال میان آمریکا، چین و اتحادیه اروپا

برای سال‌ها، جهان اینترنت به‌عنوان منطقه‌ای بی‌مرز بود که مردم را از سرتاسر جهان دور هم جمع می‌کرد. در سال‌های اولیه، طرفداران اینترنت از توانایی آن در فراتر رفتن از مرزهای ملی، برابر کردن دسترسی به اطلاعات و حتی ترویج دموکراسی خبر دادند. بسیاری پیش‌بینی کردند که هر تلاشی برای تنظیم آزادی بیان در اینترنت با شکست مواجه خواهد شد.

اکنون، دولت‌ها در سراسر جهان چارچوب‌های نظارتی بسیار متفاوتی را دنبال می‌کنند و درنتیجه رؤیای یک اینترنت واحد و رایگان در حال محو شدن است. در ایالات‌متحده، آزادی بیان و رویکرد آزادسازی منجر به موفقیت عظیمی برای شرکت‌هایی مانند اپل، گوگل و آمازون شده است. درعین‌حال، بسیاری از تحلیلگران می‌گویند، اینترنت ایالات‌متحده مملو از اطلاعات نادرست، محتوای مضر و «سرمایه‌داری نظارتی» است. در چین، دیواری بزرگ و ارتشی از مدیران محتوا، قلمرو دیجیتال را با موفقیت تحت کنترل دولت چین قرار داده‌اند. در اروپا، تنظیم‌گرها در اجرای حفاظت از حریم خصوصی داده‌ها موفقیت شگفت‌انگیزی داشته‌اند. اما ازآن‌جایی‌که دولت‌ها مسیرهای نظارتی بسیار متفاوتی را دنبال می‌کنند، اینترنت یکپارچه درحال پاشیده شدن است. در وضعیت کنونی حداقل سه اینترنت وجود دارد؛ یکی به رهبری ایالات‌متحده، یکی توسط چین و دیگری توسط اتحادیه اروپا. در یک نشست آدام سگال «AdamSegal»، آنو بردفورد «Anu Bradford» و تارا ویلر «Tarah Wheeler» پیرامون این سه مدل اینترنت، گفتگو کرده‌اند.

عنوان	The Three Internets
نویسنده	Anu Bradford, Adam Segal, Tarah Wheeler
مرکز مطالعاتی	CFR
تاریخ انتشار	December 7, 2022

تقویت همکاری ایالات‌متحده و اتحادیه اروپا در تجارت و فناوری

شورای تجارت و فناوری (TTC) که در سال ۲۰۲۱ راه‌اندازی شد، به پلتفرم اصلی همکاری ایالات‌متحده و اتحادیه اروپا در بخش اقتصاد، فناوری و امنیت تبدیل شده است. این شورا قصد دارد ازطریق جلسات دوسالانه وزیران و ۱۰ کارگروه، همکاری را تعمیق بخشد. بااین‌حال، اختلافات جدید فراآتلانتیک مانند آنچه درمورد قانون کاهش تورم ایالات‌متحده آمریکا در حال ظهور است، خطر تحت‌الشعاع قرار دادن آن را دارد.

این گزارش، اقدامات TTC تا حال حاضر را مورد ارزیابی قرار داده و بینش‌هایی درباره چگونگی توسعه TTC در کوتاه‌مدت و بلندمدت ارائه می‌دهد. همچنین چگونگی تناسب TTC در کنار سایر ساختارهای حاکمیتی متمرکز بر تجارت و فناوری را بررسی می‌کند. سپس مجموعه اقداماتی را برای تقویت TTC و پیوند آن با انجمن‌های مجاور مانند G7 توصیه می‌کند.

عنوان	Strengthening US-EU cooperation on trade and technology
نویسنده	Marianne Schneider-Petsinger
مرکز مطالعاتی	Chathamhouse
تاریخ انتشار	December 8, 2022

تأثیر انحصار و رقابت بر عرضه نرم‌افزارها

ایلان ماسک اخیرا فاش کرد اپل تهدید کرده که توییتر را از اپ‌استور حذف خواهد کرد. دو روز بعد، ماسک پس از ملاقات با تیم‌کوک «Tim Cook»، مدیرعامل اپل، در توییتی نوشت که این تهدید صرفاً یک سوءتفاهم بوده است.

به نظر می‌رسد آرمان‌های آزادی بیان ماسک برای توییتر چیزی است که این شرکت را در تیررس اپل قرار داده است. درحالی‌که ماسک ممکن است این بار از حمله اپل در امان مانده باشد، تا زمانی که انحصار اپل (در کنار گوگل) بر بازار اپلیکیشن‌ها پابرجا باشد، امکان حذف آن از فهرست نرم‌افزارها وجود خواهد داشت. این کنترل، اپل را به یکی از قدرتمندترین دروازه‌بانان اینترنت تبدیل کرده است.

به دلیل عدم‌وجود نظارت مؤثر در سیلیکون‌ولی، اپل بازار نرم‌افزارهای موبایل را تسخیر کرده و از قدرت خود برای سوءاستفاده از رقبا و سرکوب رقابت استفاده می‌کند. زمانی که توسعه‌دهندگان اپلیکیشن موبایل، برنامه‌های خود را در اپ‌استور فهرست می‌کنند، اپل آن‌ها را مجبور می‌کند تا ۳۰ درصد از تمام تراکنش‌های درون‌برنامه را به اپل بپردازند. هنگامی‌که توسعه‌دهندگان از این امر عقب‌نشینی می‌کنند، اپل می‌تواند با سرعت برنامه را از لیست خود حذف کند و مانع کسب‌وکار آن‌ها شود. سوءاستفاده اپل از توسعه‌دهندگان موبایل فقط به «مالیات اپل» محدود نمی‌شود، بلکه این شرکت همچنین از قدرت خود برای پیشبرد موقعیت‌های سیاسی استفاده می‌کند.

عنوان	Apple May Soon Have To Choose Between China's WeChat, and Elon Musk's Twitter
نویسنده	Jake Denton
مرکز مطالعاتی	Heritage
تاریخ انتشار	December 8, 2022

مطالعه‌ای در استانداردهای تیک‌تاک و توییتر

از یک طرف، ما مالک آمریکایی یک پلتفرم رسانه اجتماعی را داریم که سعی می‌کند از آن برای گسترش دامنه بحث عمومی استفاده کند، حتی اگر شامل صداهایی باشد که برخی یا بسیاری با آن مخالف هستند، و به‌راحتی می‌توان آن را به‌عنوان اطلاعات نادرست رد کرد. ازسوی دیگر، ما پلتفرمی داریم که توسط چین کنترل و توسط مهندسان چینی نگهداری می‌شود که داده‌ها را برای استفاده توسط ارتش و سرویس‌های اطلاعاتی چین جمع‌آوری می‌کند. ماه گذشته در طی یک پیش‌بینی بیان شد که تیک‌تاک و توییتر دو مدل کاملاً متضاد برای آینده رسانه‌های اجتماعی ارائه می‌دهند.

به‌عنوان مثال، ایلان ماسک درمورد کارهایی که در توییتر انجام می‌دهد، ازجمله لغو ممنوعیت کاربرانی مانند رئیس‌جمهور سابق آمریکا، ترامپ، فضا را تا حدی باز گذاشته است که به‌راحتی اطلاعات نادرست منتشر می‌شود. در آن‌سو فضای تیک‌تاک بسیار بسته است و داده‌ها را به سرویس‌های نظامی و جاسوسی چین تحویل می‌دهد تا آن‌ها ازطریق قابلیت هوش مصنوعی خود مزیت استراتژیک کسب کنند و بتوانند صدای مخالفین را خاموش نمایند.

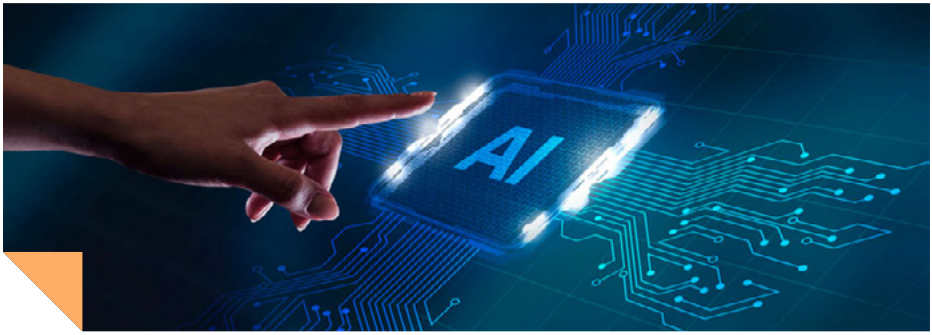
عنوان	TikTok And Twitter: A Study In Double Standards
نویسنده	Arthur Herman
مرکز مطالعاتی	Hudson
تاریخ انتشار	December 5, 2022

پیشرفت آهسته؛ ترس از آسیب‌های هوش مصنوعی را کاهش می‌دهد

با گذشت نزدیک به هفت سال از دوران یادگیری عمیق، واضح است که توسعه مزایای پیشرفت هوش مصنوعی بیشتر از آنچه پیش‌بینی می‌شد طول خواهد کشید و این به جامعه زمان زیادی می‌دهد تا به بررسی خطرات و جنبه‌های منفی این قابلیت بپردازد.

پس از دهه‌ها استفاده از روش‌های سنتی در توسعه هوش مصنوعی، متخصصان برای نوآوری گسترده به روش‌های نو دست یافته بودند که سه مؤلفه اصلی داشت؛ ۱) اینترنت حجم وسیعی از داده‌های موردنیاز برای خودآموزی را فراهم می‌کند ۲) ظهور محاسبات ابری به این معنی است که قدرت پردازش مورد نیاز، اکنون به‌آسانی و ارزان در دسترس است و ۳) وب جهانی باعث می‌شود خدمات جدید به سرعت و در سطح جهانی برای مشاغل و مصرف‌کنندگان به‌طور یکسان گسترش یابند.

در مقابل، تلاش‌های قبلی هوش مصنوعی فاقد هر سه مؤلفه بودند. به عبارتی داده‌های ناکافی، محاسبات گران‌قیمت و برنامه‌های کاربردی محدود وجود داشت. این برآوردها به معنای انتقاد از هوش مصنوعی یا نادیده گرفتن پتانسیل آن نیست، بلکه صرفاً تصدیق می‌کند که سرعت تغییر ثابت شده است. از منظر تاریخی، ظهور کامل قابلیت‌های هوش مصنوعی جدید که توان تغییر بازی را دارند، ۱۰ تا ۳۰ سال طول می‌کشد. اما با وجود این هوش مصنوعی آسیب‌هایی دارد که این گزارش به تشریح آن‌ها و ارائه راهکارهایی برای حل مسائل ناشی از آن پرداخته است.



عنوان	Slow Progress Is Taking the Fear Out of Artificial Intelligence
نویسنده	David Moschella
مرکز مطالعاتی	ITIF
تاریخ انتشار	December 2, 2022

FTC چگونه باید به تبلیغات اینترنتی فریبنده رسیدگی کند؟

تأیید محصولات از سوی افراد مشهور کوچک و بزرگ می‌تواند به فروش بیشتر آن‌ها کمک کند. اما تبلیغات فریبنده، به‌ویژه در پلتفرم‌های رسانه‌های اجتماعی و در پلتفرم‌های بررسی کالا توسط مصرف‌کنندگان، می‌تواند موجب گمراهی آن‌ها شود. تکامل سریع رسانه‌های اجتماعی و تبلیغات حمایتی چالش‌های جدیدی را نظیر نحوه افشای روابط مالی بین اینفلوئنسرها، رسانه‌های اجتماعی و برندها ایجاد کرده است. ظهور پلتفرم‌های جدید وب ۳، ازجمله متاورس، احتمالاً سؤالات جدیدی مانند قوانین مربوط به تأیید افراد مشهور مجازی ایجاد خواهد کرد. همان‌طور که کمیسیون تجارت فدرال (FTC) راهنماهای تأیید را به‌روز می‌کند، مجموعه‌ای از مثال‌ها و دستورالعمل‌های طراحی‌شده برای کمک به کسب‌وکارها جهت مطابقت با شیوه‌های تبلیغاتی موردتأیید FTC ارائه کرده است که از سال ۲۰۰۹ تاکنون برای اولین بار ارائه شده، فرصت مهمی را برای شفاف‌سازی به وجود می‌آورد.

در همین رابطه، ITIF در میزگردی با موضوع آینده راهنمای تأییدیه‌ها و اینکه چگونه پلتفرم‌ها و سیاست‌گذاران می‌توانند برای محافظت از مصرف‌کنندگان، ترویج نوآوری و بهبود تبلیغات آنلاین، مؤثر باشند، متخصصان این حوزه را دور هم جمع کرده است.

عنوان	How Should the FTC Address Deceptive Endorsement Advertising Online?
نویسنده	Irene Ly, Christopher Terry, Becca Trate, Po Yi
مرکز مطالعاتی	ITIF
تاریخ انتشار	December 8, 2022

چگونه داده‌ها بر چالش‌های سیاست جهانی تأثیر می‌گذارد؟

جمع‌آوری داده‌ها هنگام رسیدگی به مسائل جهانی مانند تغییرات آب و هوا، واکنش به بلایا و سلامت عمومی از اهمیت حیاتی برخوردار است. اما برخی از گروه‌ها به داده‌ها در ارتباط با خود و جوامع‌شان دسترسی دارند و برخی دیگر دسترسی ندارند. شکاف‌های مهم در داده‌ها مانع از اقدام مشترک درباره چالش‌های کلیدی جهانی می‌شود. به‌عنوان مثال، کشورها در کیفیت و کمیت داده‌های هواشناسی جمع‌آوری‌شده متفاوت هستند، به این معنی که مدل‌های پیش‌بینی آب‌وهوا برای یک منطقه خاص ممکن است نادرست باشد. داده‌های آب‌وهوایی با کیفیت بالا نیز برای واکنش به بلایا ضروری و به این معنی است که سیستم‌های هشدار زودهنگام برای جوامعی که در معرض خطر بیشتری هستند، اثرگذاری کمتری دارند. در همین حال، بسیاری از کشورها هنوز سال‌ها از جمع‌آوری داده‌های کافی برای دستیابی به اهداف توسعه پایدار سازمان ملل عقب مانده‌اند؛ به عبارتی برخی از کشورها می‌توانند تصمیمات مبتنی‌بر شواهد درمورد توسعه ملی اتخاذ کنند، درحالی‌که برخی دیگر فاقد اطلاعات درخصوص حوزه‌های موردنیاز خود هستند.

دراین‌راستا مرکز نوآوری داده ITIF در میزگردی به موضوع تأثیر شکاف داده‌ها بر چالش‌های بحرانی خط‌مشی جهانی و راه‌هایی که کاهش این تفاوت‌ها ممکن است به نوآوری و شکوفایی مبتنی بر داده‌های جهانی کمک کند، پرداخته است.

عنوان	How Does the Data Divide Impact Global Policy Challenges?
نویسنده	Ginette Azcona, Lizzie Coles-Kemp, Gillian Diebold, Valerie Perhirin, Oleg Petrov
مرکز مطالعاتی	ITIF
تاریخ انتشار	December 7, 2022

جمع‌آوری داده‌ها می‌تواند با نابرابری مبارزه کند

فهرست کردن تمام خطرات جمع‌آوری داده‌ها، از منظر حفظ حریم خصوصی و نظارت و از منظر عدم‌شفافیت که ملازم مالکیت داده می‌باشد، به یک نقطه گفتگوی جذاب تبدیل شده است. اما باید توجه کرد که به‌جای غرق شدن در خطرات احتمالی، زمان آن رسیده است که بدانیم چگونه فقدان جمع‌آوری داده‌ها درباره برخی افراد و جوامع می‌تواند بر کیفیت زندگی آن‌ها تأثیر منفی بگذارد.

در اقتصاد دیجیتال امروزی، یکی از موانع مهم در برابر فرصت‌ها وجود شکاف داده‌ها و نابرابری‌های اجتماعی و اقتصادی ناشی از این عدم‌جمع‌آوری و بکارگیری داده است.

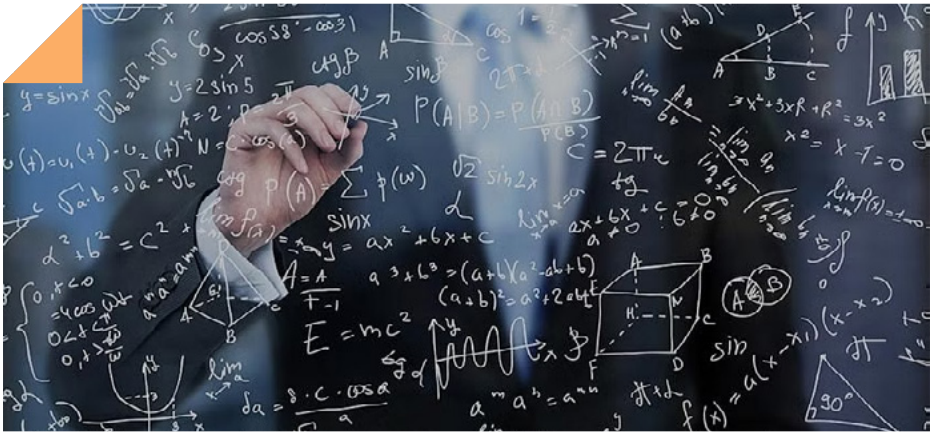
بستن شکاف داده باید یک اولویت سیاستی در ایالات‌متحده باشد تا رشدی قوی و عادلانه در اقتصاد دیجیتال ایجاد کند. داده‌ها در اقتصاد امروزی بسیار ارزشمند شده‌اند. این معنا که افراد و جوامع تا چه حد می‌توانند داده‌ها را جمع‌آوری کرده و آن‌ها را مورد استفاده قرار دهند، به تعیین همه‌چیز، از اثرگذاری در حوزه سلامت گرفته تا ایمنی عمومی و رشد اقتصادی، کمک می‌کند.

عنوان	Better Data Collection Can Fight Inequality
نویسنده	Gillian Diebold
مرکز مطالعاتی	ITIF
تاریخ انتشار	November 25, 2022

الگوریتم‌ها دشمن نیستند

تنظیم رسانه‌های اجتماعی در صدر فهرست برنامه‌های سیاست‌گذاران قرار داشته و راهکاری که از میان بسیاری از لوایح پیش‌روی کنگره ظاهر شده، مجازات یا عدم‌انگیزه استفاده از الگوریتم‌هاست. این اقدامات که برای تبدیل اینترنت به مکانی بهتر و امن‌تر طراحی شده‌اند، می‌توانند درنهایت نتیجه معکوس داشته باشند.

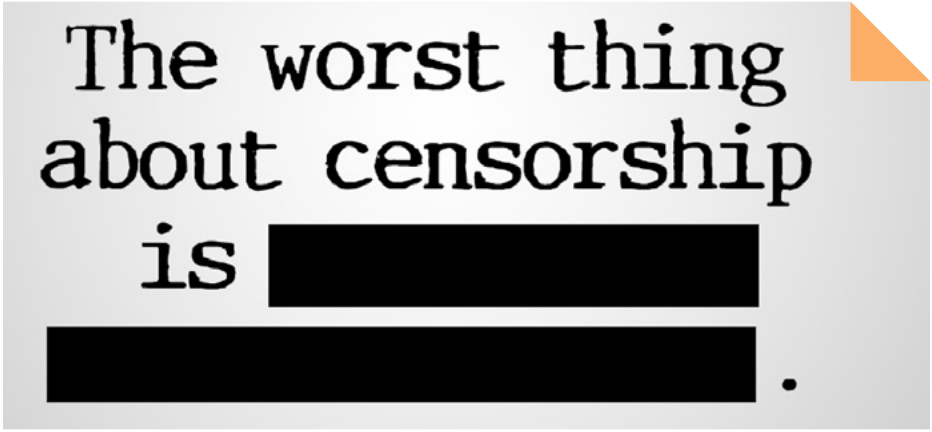
این رویکرد نتیجه استدلال منتقدانی است که می‌گویند الگوریتم‌های پلتفرم‌های رسانه‌های اجتماعی ممکن است برای سلامت روانی کاربران مضر باشند و منجر به افزایش قطبی‌سازی سیاسی یا حتی رادیکال‌سازی شوند. محور بسیاری از این استدلال‌ها این ادعاست که پلتفرم‌های رسانه‌های اجتماعی محتوای بحث‌برانگیز یا مضر را تقویت می‌کنند، یا به‌عنوان بخشی از یک طرح برای جلب توجه کاربران و نگه داشتن آن‌ها در پلتفرم به‌کار گرفته می‌شوند یا به‌طور خودکار محتوای کاربران را تقویت نموده و سعی می‌کنند مخاطب با محتوای بیشتری تعامل داشته باشد، خصوصا محتوایی که بیشتر واکنش‌های منفی را تحریک می‌کند.



عنوان	Algorithms Are Not the Enemy
نویسنده	Ashley Johnson
مرکز مطالعاتی	ITIF
تاریخ انتشار	December 8, 2022

چالش بخش ۲۳۰ قانون نجابت در آمریکا

بخش ۲۳۰ قانون نجابت انتقاداتی را به همراه داشته است؛ این انتقادات عمدتاً ازسوی قانون‌گذاران جمهوری‌خواه مطرح می‌شود که استدلال می‌کنند این قانون به پلتفرم‌های رسانه‌های اجتماعی اجازه می‌دهد دیدگاه‌های محافظه‌کارانه را سانسور کنند؛ پس لایحه‌های متعددی از سوی ایشان ارائه شد که به دنبال تغییر بخش ۲۳۰ است. برخی محافظه‌کاران می‌خواهند بخش ۲۳۰ را لغو یا آن را اصلاح کنند تا محدودیت‌هایی را برای حذف غیرمسئولانه انداع محتوا در سرویس‌های آنلاین ایجاد کنند. دومین نکته در صورت حذف بخش ۲۳۰، نه‌تنها مانع از توانایی سرویس‌های آنلاین برای تعدیل محتوا می‌شود، بلکه سرویس‌های آنلاین مجبور به حذف هر محتوایی خواهند شد که کوچک‌ترین شبهه‌ای درباره آن وجود داشته باشد؛ ازجمله حذف انواع محتوایی که در یک منطقه خاکستری پیچیده قرار می‌گیرند که به‌طور گسترده مضر و درعین‌حال غیرقانونی تلقی می‌شوند. درنتیجه، لغو بخش ۲۳۰ احتمالاً منجر به سانسور بیشتر خواهد شد، زیرا خدمات آنلاین انگیزه بیشتری برای حذف هرگونه محتوایی خواهند داشت که به‌طور بالقوه می‌تواند آن‌ها را در مشکلات قانونی قرار دهد، از جمله محتوای بحث‌برانگیز مانند گفتمان سیاسی.

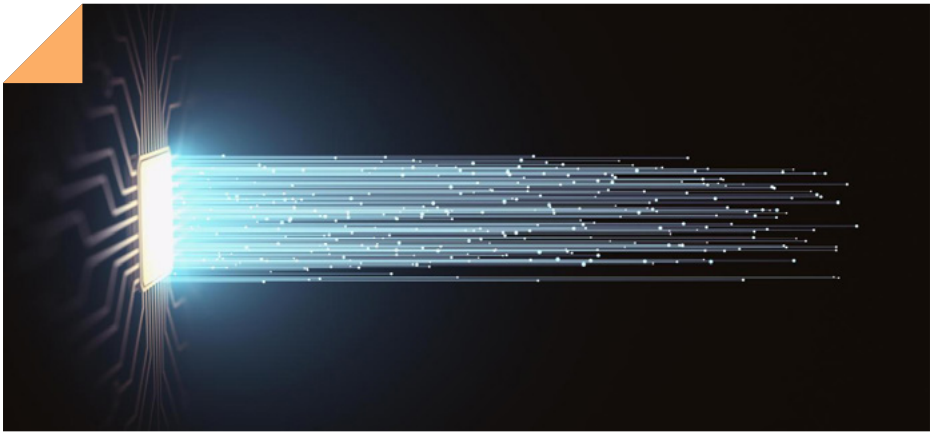


عنوان	Section 230 Still Isn't the Solution to Conservative Claims of Social Media Censorship
نویسنده	Ashley Johnson
مرکز مطالعاتی	ITIF
تاریخ انتشار	December 6, 2022

نوروتکنولوژی چیست؟

وقتی اکثر مردم به پیشرفت‌های پزشکی فکر می‌کنند، توسعه دارو اولین چیزی است که به ذهنشان می‌رسد. درحالی‌که فناوری نو، ابزارهای ارزشمندی برای درمان بیماری‌های صعب‌العلاج هستند. راه‌حل‌های فناوری در زمینه عصب‌شناسی در حال بروز و ظهور هستند، زیرا این پتانسیل را دارند که به‌طور خاص یک نوع بیماری را به روش‌هایی درمان کنند که داروها نمی‌توانند. نوروتکنولوژی به‌طور گسترده به‌عنوان یک فناوری طراحی‌شده برای بهبود و ترمیم عملکرد سیستم عصبی و همچنین برای توانمندسازی محققان و پزشکان برای تجسم مغز شناخته می‌شود. نمونه‌هایی از فناوری عصبی در فرهنگ عامه عبارت است از ایجاد رابط مغز و ماشین و اسکنر مغز. دستگاه‌های نوروتکنولوژی به تسکین درد کمک کرده، ایده عملکرد مغز را در اختیار پزشکان قرار می‌دهند و مغز را برای درمان بیماری پارکینسون تحریک می‌کنند.

اگرچه فناوری که به‌سرعت در حال تغییر است، نویدهای زیادی را برای افرادی که با طیف وسیعی از بیماری‌ها زندگی می‌کنند، ارائه می‌دهد، اما سرمایه‌گذاری در حوزه نوروتکنولوژی در گرو درنظر گرفتن ابعاد مختلف ازجمله زیست‌شناسی، مهندسی، تنظیم دستگاه و روندهای کلان در بازار است. این گزارش که توسط بنیاد برایت فوکوس «BrightFocus» تأمین مالی شده است، کاربردهای بالقوه، فرصت‌ها و موانع را برای کمک به هدایت نقش محوری بشردوستی در پیشبرد این زمینه بررسی می‌کند.



عنوان	Neurotechnology: A Giving Smarter Guide
نویسنده	Sylvie Raver, Elena Helmers-Wegman, Cara Altimus
مرکز مطالعاتی	Milkeninstitute
تاریخ انتشار	December 9, 2022

اولویت‌های امنیت سایبری هند برای ریاست G20

ابتدای دسامبر ۲۰۲۲، هند ریاست G20 متشکل از اقتصاد بزرگ جهان را بر عهده گرفت. با بهبود وضعیت اقتصادی پس از همه‌گیری کرونا و افزایش تنش‌های ژئوپلیتیکی، به دلیل مناقشه روسیه و اوکراین، اولویت‌های گروه ۲۰ در دو سال گذشته تغییر کرده است. بااین‌حال، برای هند، موضوعاتی مانند زیرساخت‌های عمومی دیجیتال، تغییرات آب‌وهوایی، انعطاف‌پذیری زنجیره تأمین و چندجانبه‌گرایی اصلاح‌شده بر دستورکار غالب خواهند بود. هند با استفاده از ظرفیت ریاست گروه ۲۰ می‌تواند ابتکارات را در زمینه‌های حیاتی سایبری، هدایت کند.

افزایش همکاری امنیت سایبری در مجمع G20 می‌تواند به تضمین امنیت و یکپارچگی زیرساخت‌های حیاتی و پلتفرم‌های عمومی دیجیتال کمک کند. بنابراین، امنیت سایبری باید یک حوزه تمرکز کلیدی در حوزه دیجیتال تحت ریاست هند در سال ۲۰۲۳ باشد.

عنوان	India's cybersecurity priorities for G20 Presidency
نویسنده	Arjun Gargeyas, Sameer Patil
مرکز مطالعاتی	ORFonline
تاریخ انتشار	December 4, 2022

آسیب‌پذیری‌های سایبری هند

فراوانی و اهداف حملات سایبری به هند به‌طور قابل‌ملاحظه‌ای جدی شده است. در اوایل ماه نوامبر، خدمات سپرده‌گذاری مرکزی هند (Central Depository Services (India) Limited یا CDSL) یک بدافزار را در برخی از ماشین‌های داخلی خود شناسایی کرد. اگرچه CSDL ادعا کرد که «هیچ دلیلی وجود ندارد که باور کنیم اطلاعات محرمانه یا داده‌های سرمایه‌گذار به خطر افتاده است؛ اما در جدیدترین حمله، یکی از برترین مؤسسات پزشکی هند - موسسه علوم پزشکی سراسر هند (AIMS) مورد حمله سایبری قرار گرفت. هرچند هند توجه بیشتری به امنیت سایبری داشته است، اما افزایش تعداد حملات به این کشور باید برای مدیران امنیتی هند بسیار نگران‌کننده باشد.

به نظر می‌رسد این حمله سایبری بر عملیات AIIMS که تقریباً یک دهه پیش کاملاً آنلاین شده بود، تأثیر گذاشته است. این حمله به تمام فایل‌های ذخیره‌شده در سرورهای اصلی و پشتیبان بیمارستانی هند، آسیب رساند. بر اساس گزارش‌ها، مجرمان موفق شدند داده‌های حساس و پرونده‌های پزشکی را برای «دریافت باج» به دست آورند. این حمله احتمالاً شامل مقامات ارشد دولتی نیز می‌شود که از AIIMS استفاده می‌کنند. این پایگاه داده شامل «اطلاعات شناسایی شخصی (PII) بیماران و کارکنان مراقبت‌های بهداشتی و سوابق اداری مربوط به اهداکنندگان خون، آمبولانس‌ها، واکسیناسیون، مراقبان و اعتبارنامه ورود کارکنان بوده است». باتوجه به ابعاد این حمله، پلیس دهلی، وزارت امور داخله و آژانس تحقیقات ملی (NIA) به تحقیقات در ارتباط با این موضوع پیوسته‌اند.

عنوان	The AIIMS cyberattack reflects India's critical vulnerabilities
نویسنده	Rajeswari (Raji) Pillai Rajagopalan
مرکز مطالعاتی	ORFonline
تاریخ انتشار	December 3, 2022

هند
درعصردیپلماسی‌سیلیکونی

کمبود جهانی نیمه‌هادی‌ها که در طول همه‌گیری کرونا رخ داد، منجر به خسارات سنگینی برای بسیاری از بخش‌های اقتصادی شد. شکنندگی زنجیره تأمین و وابستگی‌های ذاتی در داخل، همکاری نیمه‌هادی‌ها را برای حفظ کارایی صنعت ضروری کرده است. این خلاصه‌نوشت به بررسی این موضوع می‌پردازد که چگونه نیمه‌هادی‌ها به نقطه اتکایی برای ایجاد اتحادهای بالقوه فناوری تبدیل شده‌اند. این نوشته همچنین، ابتکارات دیپلماتیک در حال انجام با هدف ایمن‌سازی زنجیره‌های تأمین جهانی و کاهش وابستگی بیش‌ازحد اکوسیستم به چین را تشریح و در این زمینه مسیر آینده هند را بررسی می‌کند.

عنوان: India in the Era of Silicon Diplomacy
نویسنده: Arjun Gargeyas
مرکزمطالعاتی: ORFonline
تاریخ انتشار: December 6, 2022

چگونگی تأثیر رسانه‌های اجتماعی بر دموکراسی و جامعه

در اقتصادهای پیشرفته و نوظهور، دیدگاه‌های مشابهی درمورد چگونگی تأثیر رسانه‌های اجتماعی بر دموکراسی و جامعه وجود دارد. براساس نظرسنجی جدید مرکز تحقیقات پیو، مردم در اقتصادهای پیشرفته احساسات متفاوتی درخصوص تأثیر رسانه‌های اجتماعی بر زندگی دارند. اکثریت مردم در ۱۹ کشور می‌گویند نقش رسانه‌های اجتماعی به دستکاری و تفرقه در جوامع منجر شده است.

در اقتصادهای نوظهور، دیدگاه‌ها درمورد این موضوعات چندان متفاوت نیست. در سال ۲۰۱۸، اکثریت ۱۱ اقتصاد نوظهور و درحال توسعه گفتند که رسانه‌های اجتماعی دارای جنبه‌های مثبت و منفی هستند. نتایج این دو نظرسنجی علی‌رغم تفاوت در زمینه و زمان، از جهات دیگر مشابه است. در شش موضوع مورد بررسی، در ۱۹ اقتصاد پیشرفته و ۱۱ اقتصاد نوظهور درباره رسانه‌های اجتماعی، سیاست و دموکراسی وحدت نظر وجود دارد.

عنوان	In advanced and emerging economies, similar views on how social media affects democracy and society
نویسنده	Laura Silver , Laura Clancy
مرکز مطالعاتی	Pew
تاریخ انتشار	December 6, 2022

تأثیر مقررات بر کریپتوکارنسی

آشفتگی در بخش کریپتو، با فروپاشی چندین پلتفرم پرمخاطب، سؤالاتی اساسی درمورد پایداری بازارهای رمزنگاری غیرقابل تنظیم ایجاد کرده است. گزینه‌های روی میز رژیم‌هایی که نظارت‌های شدید بر مردم دارند، برای مقابله با این مسئله چیست؟ و آیا آن‌ها می‌توانند بخش کریپتو را تنظیم کنند؟ مرکز مطالعاتی پیترسون طی نشستی این سؤالات را مورد بررسی قرار داده است. میزبان این نشست نیکلاس ورون «Nicolas V ron» (عضو ارشد موسسه اقتصاد بین‌الملل PIIE) بوده و متیو الدرفیلد «Matthew Elderfield» (معاون سابق رئیس بانک مرکزی ایرلند) و کارن پترو «Karen Petrou» (مدیریت تجزیه‌وتحلیل مالی فدرال آمریکا) به‌عنوان مهمان در این نشست شرکت کردند.

عنوان	Can regulation save crypto?
نویسنده	Matthew Elderfield, Karen Petrou
مرکز مطالعاتی	PIIE
تاریخ انتشار	December 13, 2022

امکان‌سنجی حملات خصمانه در برابر هوش مصنوعی

حجم وسیعی از ادبیات دانشگاهی تعداد بی‌شماری از حملات به هوش مصنوعی را برشمرده و نشان می‌دهد که بیشتر سیستم‌های هوش مصنوعی وزارت دفاع ایالات‌متحده در خطر دائمی حمله قرار دارند. بااین‌حال، محققان مؤسسه رند برخی از حملات خصمانه را بررسی کرده و دریافتند که طراحی و استقرار بسیاری از حملات ازنظر عملیاتی غیرممکن است، زیرا باتوجه‌به نیاز دانش بالا، این امر غیرعملی است. همان‌طور که محققان در این گزارش بحث می‌کنند، تکنیک‌های غیرخصمانه آزمایش‌شده و واقعی‌ای وجود دارد که می‌تواند ارزان‌تر، عملی‌تر و اغلب مؤثرتر باشد. با وجود این، سیستم‌های هوش مصنوعی خوبی طراحی شده که خطرات چنین حملاتی را کاهش می‌دهد. همچنین ترکیب داده‌ها و پیش‌بینی‌ها در روش‌های حسگر، نمونه‌برداری سیگنال و وضوح تصویر می‌تواند خطر حملات خصمانه علیه هوش مصنوعی را کاهش دهد.

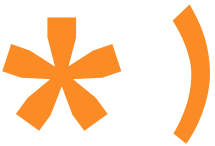
عنوان	Operational Feasibility of Adversarial Attacks Against Artificial Intelligence
نویسنده	Li Ang Zhang, Gavin S. Hartnett, Jair Aguirre, Andrew J. Lohn, Inez Khan, Marissa Herron, Caolionn O'Connell
مرکز مطالعاتی	Rand
تاریخ انتشار	December 12, 2022

آینده همکاری فضایی بین ایالات متحده و ژاپن

کارشناسان و متخصصان، چشم‌انداز خود را برای آینده علم و اکتشاف فضایی، همکاری بین ایالات‌متحده و ژاپن و اقتصاد فضایی آینده ارائه کردند. این ویدئوها شامل دیدگاه‌هایی است که به‌صورت حضوری در دفتر مرکزی مؤسسه رند در سانتا مونیکا برگزار و به‌صورت زنده پخش شد.

موضوع روز اول این رویداد «دیدگاه‌های ایالات‌متحده و ژاپن از آینده علم و اکتشاف فضایی» بود و سخنرانی اصلی توسط دکتر دیوید کیپینگ «David Kipping»، استادیار نجوم و مدیر آزمایشگاه دانشگاه کلمبیا انجام شد. سایر سخنرانان عبارتنداز: دکتر کریستین جانسون«Christian Johnson»، دانشیار اطلاعات شرکت رند، آقای شو ناکانوسه«Sho Nakanose»، بنیان‌گذار و مدیرعامل GITAI؛ و دکتر پیت وردن«Pete Worden»، مدیر اجرایی استارشات «Starshot» و مدیر سابق مرکز تحقیقات ایمز ناسا «NASA Ames Research Center».

موضوع روز دوم «دیدگاه‌های ایالات‌متحده و ژاپن درمورد همکاری‌های علوم فضایی و اقتصاد فضایی آینده» بود و سخنرانی اصلی توسط آقای ایشی یاسو «Ishii Yasuo»، معاون آژانس اکتشافات هوافضای ژاپن (JAXA) برای همکاری‌های بین‌المللی ارائه شد.



عنوان	The Future of Space Cooperation Between the U.S. and Japan
نویسنده	David Kipping, Christian Johnson, Sho Nakanose, Pete Worden, Ishii Yasuo, Bonnie L. Triezenberg, Chad J. R. Ohlandt, Ron Lopez, Isaac Arthur, Scott W. Harold
مرکز مطالعاتی	Rand
تاریخ انتشار	December 7, 2022

حفاظت و ایمن‌سازی داده‌ها در برابر تهدید کوانتومی

در طول دهه آینده، محاسبات کوانتومی پیشرفت‌های فناوری جدید را پیش‌روی ما باز کرده و چشم‌انداز امنیتی کنونی را متحول خواهد کرد. کاخ سفید در ماه می هشدار داد که کامپیوترهاي کوانتومي با اندازه و پيچيدگي كافي مي‌توانند ارتباطات غيرنظامي و نظامي را به خطر بيندازند، سيستم‌هاي نظارتي و كنترلي زيرساخت‌هاي حياتي را تضعيف كنند و پروتكل‌هاي امنيتي را براي اغلب تراكنش‌هاي مالي مبتني‌بر اينترنت از بين ببرند. در گزارش جداگانه‌ای از مرکز ملی ضدجاسوسی و امنیت، این هشدار آمده است: «هرکسی که در رقابت برای برتری محاسبات کوانتومی پیروز شود، می‌تواند ارتباطات دیگران را به خطر بیندازد.»

هنگامی که یک کامپیوتر کوانتومی به‌اندازه‌ای پیچیده و بزرگ می‌شود که تهدیدی برای رمزگذاری مدرن به حساب می‌آید، به آن رایانه کوانتومی مرتبط با رمزنگاری یا «CRQC» می‌گویند. برخی از کارشناسان انتظار دارند محاسبات کوانتومی ظرف سه سال آینده به خطری برای رمزگذاری مدرن تبدیل شود، اگرچه دیگران این اتفاق را بالای بیست سال برآورد کرده‌اند.

دو راه برای تأمین امنیت در برابر تهدید کوانتومی وجود دارد. مؤسسه ملی استانداردها و فناوری (NIST) رویکرد «عدم‌امکان محاسباتی» را اتخاذ کرده است، که هدف آن توسعه رمزگذاری با چنان پیچیدگی است که قدرت محاسباتی کوانتومی نیز توان نقض آن را ندارد. برای این منظور، NIST در حال تحقیق و آزمایش الگوریتم‌های جدید و توسعه استانداردهای رمزگذاری پَس‌کوانتومی است که باید تا سال ۲۰۲۴ به نتیجه برسد. بااین‌حال، اگر این فناوری محقق نشود، در صورت ظهور CRQC در چند سال آینده، بسیاری از کاربران در برابر نفوذهای سایبری آسیب‌پذیر خواهند شد.

عنوان	Protecting and Securing Data from the Quantum Threat
نویسنده	Georgianna Shea, Annie Fixler
مرکز مطالعاتی	FDD
تاریخ انتشار	December 16, 2022

همکاری آمریکا و فرانسه برای ایمن‌سازی دارایی‌های مجازی

رئیس‌جمهور آمریکا، جو بایدن، در بیانیه‌ای مشترک با امانوئل مکرون، رئیس‌جمهور فرانسه، متعهد به تقویت امنیت سایبری سیستم‌های مجازی تجاری شد. آسیب‌پذیری این سیستم‌ها از ویژگی‌های فیزیکی و فنی آن‌ها و همچنین رویکرد پراکنده دولت ایالات‌متحده به مدیریت ریسک ناشی می‌شود.

ایالات‌متحده و فرانسه با درک استفاده روبه‌رشد از قابلیت‌های فضای تجاری برای حمایت از عملکردهای حیاتی؛ برای امنیت ملی، ثبات اقتصادی و امنیت عمومی متعهد شدند که همکاری دوجانبه را برای افزایش انعطاف‌پذیری سایبری سیستم‌های مجازی افزایش دهند. این بیانیه منعکس‌کننده استراتژی امنیت ملی دولت بایدن است که دولت ایالات‌متحده را متعهد می‌کند «تاب‌آوری سیستم‌های مجازی ایالات‌متحده را که برای عملکردهای حیاتی امنیت ملی و داخلی به آن‌ها تکیه می‌کنیم، افزایش دهد». سیستم‌های مجازی برای امنیت ملی، رفاه اقتصادی و فعالیت روزانه شهروندان آمریکایی حیاتی هستند. برای مثال، خدمات سیستم‌های موقعیت‌یاب جهانی (GPS) نه‌تنها سیستم‌های ناوبری اتومبیل، بلکه عملکرد دارایی‌های نظامی ایالات‌متحده و زمان‌بندی تراکنش‌های خودپرداز را نیز فعال می‌کند. بنابراین، صنعت فضای تجاری یکی از سریع‌ترین صنایع در حال رشد امروزی است که بیش از ۴۴۰ میلیارد دلار فعالیت اقتصادی در سال ۲۰۲۰ ایجاد می‌کند و پیش‌بینی می‌شود در ۱۰ تا ۱۵ سال آینده از ۱ تریلیون دلار فراتر رود.

دشمنان آمریکا اهمیت سیستم‌های مجازی تجاری را درک کرده و حملات سایبری را - گاهی ازطریق نیروهای نیابتی - برای تخریب یا نابود کردن آن‌ها آغاز کرده‌اند. در اکتبر ۲۰۲۲، کنستانتین ورونتسوف «Konstantin Vorontsov»، یک مقام ارشد وزارت خارجه روسیه هشدار داد که اگر آمریکا به حمایت از اوکراین ادامه دهد، ماهواره‌های تجاری ممکن است به یک هدف تلافی‌جویانه تبدیل شوند. درواقع هکرهای روسی قبلاً این سیستم‌ها را هدف قرار داده‌اند. تنها یک ساعت قبل از حمله نیروهای مسلح این کشور به اوکراین در ماه فوریه، دولت روسیه شرکت ماهواره‌ای ویاسات مستقر در ایالات‌متحده را هک کرد و ارتباطات نظامی اوکراین و همچنین سرویس اینترنت در سراسر اروپا را مختل نمود. پیش‌ازاین، در سال ۲۰۱۸، هکرهای روسی سیستم ماهواره‌ای ناوبری جهانی (GNSS) را هدف قرار دادند و مختصات و داده‌های ناوبری معیوب را ارسال کردند تا ازطریق تکنیک‌های پارازیت و جعل، حرکت هزاران هواپیما و کشتی را مختل کنند. در همین حال، چین در حال آزمایش توانایی‌ها برای حمله به ماهواره‌های متخاصم ازطریق جنگ سایبری و الکترونیکی است.

عنوان	U.S.-French Commitment to Secure Space Assets Shines a Light on Cyber Vulnerability
نویسنده	Annie Fixler
مرکز مطالعاتی	FDD
تاریخ انتشار	December 7, 2022

آیا واشنگتن همانند چین، یک طرح کمپین فضای مجازی دارد؟

طبق گزارش وزارت خزانه‌داری، برآورد می‌شود که پرداخت‌های باج افزار در سال ۲۰۲۱ بیش از یک میلیارد دلار برای شرکت‌های آمریکایی هزینه داشته باشد. اما این رقم خیره‌کننده در مقایسه با صدها میلیارد دلار دارایی معنوی که چین هر سال از مشاغل آمریکایی به سرقت می‌برد، کمرنگ است.

در طول ۱۸ ماه از ژوئن ۲۰۱۷، یک دانشمند چینی به‌تنهایی اطلاعات اختصاصی به ارزش یک میلیارد دلار را از کارفرمای خود به سرقت برد. گستردگی عملیات هک جهانی چین، پکن را به یک حریف سرسخت تبدیل کرده است. اما تاکتیک‌هایی است که هکرهای چینی به کار می‌گیرند - نفوذ به زنجیره‌های تأمین و اکوسیستم زیرساختی اقتصاد دیجیتال - که به‌طور تصاعدی فرصت‌های بیشتری را برای تضعیف اقتصاد و امنیت ایالات‌متحده در اختیار پکن قرار می‌دهد.

کمیسیون بازنگری اقتصادی و امنیتی ایالات‌متحده و چین در گزارش سالانه ۲۰۲۲ خود هشدار داد که در دهه گذشته، «چین درگیر افزایش گسترده قابلیت‌های سایبری خود بوده است». در این گزارش هشدار داده شد که عملیات سایبری چین هدفمندتر، چابک‌تر و خطرناک‌تر است، زیرا پکن بر ساخت شخص ثالث برای نفوذ به شبکه‌های قربانیان تکیه کرده است. همان‌طور که مایکروسافت در گزارش سالانه دفاع دیجیتال خود در سال ۲۰۲۲ توضیح داد، به‌جای توسعه ده‌ها طرح جنگی مختلف برای حمله به قربانیان، هکرهای چینی یک ارائه‌دهنده خدمات فناوری اطلاعات و دسترسی آن به فروشنده را به خطر می‌اندازند تا صدها مشتری مستقیم و هزاران مشتری غیرمستقیم را آلوده کنند. جامعه اطلاعاتی ایالات‌متحده در آوریل ۲۰۲۱ به این نتیجه رسید که پکن به شرکت‌های مخابراتی، ارائه‌دهندگان خدمات مدیریت‌شده و نرم‌افزارهای پرکاربرد، و سایر اهدافی که دارای فرصت‌های بالقوه بعدی برای جمع‌آوری اطلاعات، حمله یا عملیات هستند، نفوذ می‌کند.

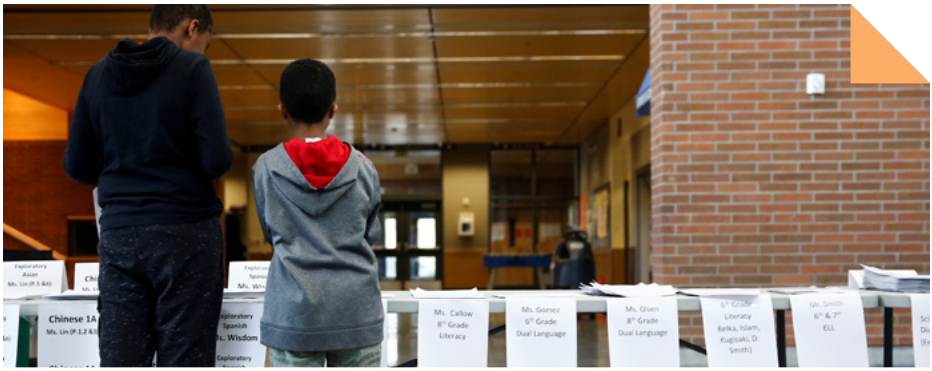
عنوان	China has a cyberspace campaign plan. Does Washington?
نویسنده	RADM (Ret) Mark Montgomery, Annie Fixler
مرکز مطالعاتی	FDD
تاریخ انتشار	December 5, 2022

تبعیض دیجیتالی چیست؟

در دسامبر امسال، کمیسیون ارتباطات فدرال (FCC) آماده است تا برای مبارزه با تبعیض دیجیتال اقدام کند. دسترسی عادلانه به پهنای باند یک هدف مهم است و این آژانس مؤظف است تضمین کند که ارتباطات از راه دور «بدون تبعیض نژادی، مذهبی، ملیتی و جنسیتی» در دسترس همه قرار می‌گیرد. اما یک سؤال کلیدی این است که «تبعیض» را چگونه تعریف می‌کنیم؟ گستردگی تعریف پیشنهادی آژانس می‌تواند پیامدهای ناخواسته‌ای برای صنعت مخابرات و به‌طورکلی برای قانون ضدتبعیض داشته باشد.

در سال ۱۹۹۶، کنگره قانون ارتباطات را اصلاح کرد تا ضدیت با تبعیض را به‌عنوان بخشی از سیاست مخابراتی آمریکا در نظر بگیرد. قانون سرمایه‌گذاری زیرساخت و مشاغل، سال گذشته این ابتکار را تقویت کرد و به FCC دستور داد تا قوانینی را برای تسهیل دسترسی برابر به پهنای باند، با جلوگیری از تبعیض دیجیتالی اتخاذ کند. برای انجام این مأموریت، FCC اطلاعیه‌ای را درخصوص قوانین پیشنهادی در دستورکار جلسه علنی ۲۱ دسامبر خود قرار داد.

شاید مهم‌ترین تصمیم آژانس نحوه تعریف «تبعیض» باشد که کنگره آن را به صلاح‌دید آژانس واگذار کرد. در ادبیات روزمره این اصطلاح به معنای تصمیم عمدی برای رفتار متفاوت با مردم براساس یک دلیل ناگفتنی است. مریام وبستر «Merriam-Webster» تبعیض را به‌عنوان «دیدگاه، اقدام یا رفتار تعصب‌آمیز» یا «عمل یا نمونه‌ای از تبعیض قاطعانه و نه فردی» تعریف می‌کند.



عنوان	What Do We Mean When We Say Digital Discrimination?
نویسنده	Daniel Lyons
مرکز مطالعاتی	AEI
تاریخ انتشار	December 14, 2022

قانون بازارهای منبع‌باز به توسعه‌دهندگان نرم‌افزار آسیب می‌رساند

حامیان مالی برنامه‌های منبع‌باز ادعا می‌کنند که اپل و آلفابت - دو ارائه‌دهنده برتر پلتفرم‌های گوشی‌های هوشمند - رقابت شرکت‌های برنامه‌های نوپا را سرکوب می‌کنند و با ناامید کردن نوآوری و افزایش مصنوعی قیمت‌ها، به مصرف‌کنندگان آسیب می‌رسانند. با هدف قرار دادن اپل، حامیان مالی ادعا می‌کنند که این شرکت با ممانعت از دسترسی به فروشگاه‌های برنامه شخص ثالث در دستگاه‌های آیفون، رقابت را خفه کرده است و توسعه‌دهندگان برنامه را ملزم به استفاده از سیستم پرداخت اپل نموده و توسعه‌دهندگان اپلیکیشن را برای اطلاع دادن به کاربران درباره پیشنهادات دارای تخفیف جریمه می‌کند.

از آن‌سو، شرکت‌های بزرگ این ادعاها را رد کرده و بیان می‌کنند که با شواهد موجود سازگار نیست. صنعت گوشی‌های هوشمند به‌قدری خوب عمل می‌کند که تعداد کاربران گوشی‌های هوشمند در ایالات‌متحده از سال ۲۰۱۶ تا ۲۰۲۱؛ ۲۵ درصد رشد داشته است و اکنون ۸۵ درصد از بزرگسالان آمریکایی از تلفن‌های هوشمند استفاده می‌کنند. حدود هفت میلیون اپلیکیشن روی پلتفرم‌های اپل و اندروید وجود دارد. حدود ۶۰۰۰ توسعه‌دهنده اپلیکیشن در ایالات‌متحده وجود دارد - تقریباً دو برابر تعداد آن‌ها در سال ۲۰۱۶ - و کسب‌وکار آن‌ها در سال ۲۰۲۲؛ ۱۲٫۶ درصد رشد کرد که از نرخ رشد سالانه ۱۰٫۵ درصدی از سال ۲۰۱۷ بیشتر است. این صنعت به سختی سرکوب شده است. بنابراین، حامیان مالی چه مدرکی برای ادعاهای خود دارند؟

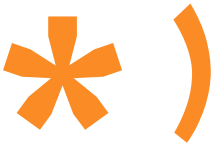
عنوان	New Evidence That the Open App Markets Act Would Harm App Developers and Innovation
نویسنده	Mark Jamison
مرکز مطالعاتی	AEI
تاریخ انتشار	December 12, 2022

مرور یک سال سایبری

یک سال پیش، جامعه جهانی امنیت سایبری به سال ۲۰۲۱ به‌عنوان سال باج‌افزار نگاه می‌کرد، زیرا تعداد حملات نسبت به سال گذشته تقریباً دو برابر شده بود و شامل اهداف برجسته‌ای مانند خط لوله استعماری می‌شد که توجه رسانه‌ها و سیاست‌ها را به این موضوع جلب کرد. اکنون و با گذشت یک سال، افزایش باج‌افزارها کند نشده است، زیرا با وجود ابتکارات کاخ سفید و آژانس امنیت سایبری و امنیت زیرساخت (CISA)، تعداد حملات به رکورد جدیدی - ۸۰ درصد در سال ۲۰۲۱ - رسیده است. تداوم حملات باج‌افزار نشان می‌دهد که این چالش تنها توسط یک دولت حل نمی‌شود، بلکه ازطریق همکاری با دوستان، رقبا و مخالفان برطرف خواهد شد.

تهاجم تمام‌عیار روسیه به اوکراین و توسعه تاریخی ۲۰۲۲، نشان می‌دهد که این چالش احتمالاً برای مدتی حل‌نشده باقی خواهد ماند. تقریباً سه‌چهارم کل درآمد باج‌افزارها به گروه‌های هکر مرتبط با روسیه بازمی‌گردد و بعید به نظر می‌رسد که همکاری با کرملین برای مقابله با این گروه‌ها به این زودی‌ها پیشرفت زیادی داشته باشد. افشاگری‌های پس از تهاجم روسیه این ظن را تأیید کرد که سرویس‌های اطلاعاتی روسیه نه‌تنها گروه‌های باج‌افزار را تحمل می‌کنند، بلکه به برخی از آن‌ها دستور مستقیم می‌دهند.

باج‌افزار تنها مسئله سایبری برای تعریف سال ۲۰۲۲ نبود، زیرا چالش‌های دیگر از فناوری عملیاتی گرفته تا توسعه نیروی کار ادامه یافت و سازمان‌های مختلف دولتی و خصوصی پیشرفت‌های قابل‌توجهی در مقابله با آن‌ها داشتند. شورای آتلانتیک گروهی از کارشناسان را گرد هم آورد تا فراز و فرودهای سال را در امنیت سایبری بررسی کرده و منتظر سال ۲۰۲۳ باشیم.



عنوان: The 5x5-The cyber year in review
نویسنده: Rep. Jim Langevin, Wendy Nather, Sarah Powazek, Megan Samford, Gavin Wilde
مرکز مطالعاتی: Atlanticcouncil
تاریخ انتشار: December 14, 2022

اهمیت ائتلاف آزادی آنلاین

برای بسیاری این باور نهادینه شده که یکی از مهم‌ترین چالش‌های زمانه ما این است که چگونه می‌توانیم از فناوری دیجیتال به شیوه‌هایی بهره ببریم که از حقوق بشر محافظت کرده تا ارزش‌های دموکراتیک مشترک حفظ شود. رئیس ائتلاف آزادی آنلاین (Freedom Online Coalition یا FOC) در سال ۲۰۲۲ بیان می‌کند: برای ما در کانادا واضح است که FOC، ائتلاف چندجانبه برای ساختن آینده‌ای که پیشرفت دیجیتال به نفع همه را مدنظر قرار دهد، نقش بزرگی در پاسخ به این چالش دارد. کانادا مفتخر است که دیدگاه جمعی از دموکراسی را در عصر دیجیتال مبتنی‌بر عناصر دیجیتالی ارتقاء داده است.

چهار مؤلفه اساسی برای دیجیتال خواندن یک کشور باید وجود داشته باشد؛ اتصال، سواد دیجیتال، مشارکت مدنی، و ایمنی آنلاین. اتصال بیشتر برای پر کردن شکاف‌های دیجیتال در سراسر جهان؛ سواد دیجیتال برای اطمینان از اینکه کاربران برای پیمایش محتوای متنوع آنلاین قدرت دارند؛ مشارکت مدنی عاری از سخنان نفرت‌انگیز و اطلاعات نادرست، سانسور محدودکننده بی‌رویه، تعطیلی اینترنت و سایر اعمال ظالمانه؛ و ایجاد یک اکوسیستم آنلاین امن برای همه.

به‌طورکلی برخورداری از عناصر دیجیتال به ما امکان می‌دهد جهانی را تصور کرده و شروع به پیشرفت کنیم که در آن رشد دیجیتال به نفع همه باشد. ائتلاف آزادی آنلاین وسیله‌ای ایده‌آل برای این اقدام جمعی است. این امر توسط دموکراسی‌های هم‌فکر هدایت می‌شود و جامعه مدنی، صنعت و متخصصین دانشگاهی ازطریق شبکه فعال مشاوران قدرت می‌گیرند. قدرت کنش جمعی نشان داده است که در میان انحطاط دموکراتیک و افزایش اقتدارگرایی دیجیتال، FOC همچنان نقشی محوری در ترویج رویکرد مبتنی بر حقوق بشر در حکمرانی فناوری‌های دیجیتال و اینترنت ایفا می‌کند.

عنوان: Canadian Deputy Foreign Minister David Morrison and US Deputy National Security Advisor Anne Neuberger on the importance of the Freedom Online Coalition
نویسنده: David Morrison, Anne Neuberger
مرکز مطالعاتی: Atlanticcouncil
تاریخ انتشار: December 13, 2022

خلاصه رویداد سیاست‌گذاری در وب۳

مرکز بلفر در ۱ دسامبر، سومین و آخرین پنل خود را در زمینه سیاست‌گذاری وب۳ به‌عنوان بخشی از دیدگاه‌های سه قسمتی خود در سری مجازی «Web۳» میزبانی کرد. محققین حقوقی، حقوقدانان و محققان سیاستی که در این حوزه کار می‌کنند، ازجمله پریماورا فیلیپی «Primavera De Filippi»، مدیر تحقیقات مرکز ملی تحقیقات علمی و دانشیار در مرکز برکمن کلین هاروارد، کانر اسپلیسی «Connor Spelliscy»، مدیر اجرایی گروه تحقیقاتی DAO، مایلز جنینگز «Miles Jennings»، مشاور عمومی و رئیس مرکز غیرمتمرکز کریپتو؛ دیوید کر «David Kerr»، و لیندسی کلهر «Lindsey Kelleher»، مدیر ارشد سیاست در انجمن بلاک‌چین حضور داشتند.

در اینجا به نکات کلیدی از این رویداد اشاره می‌شود:

۱. نیاز روزافزونی به نظارت بیشتر پیرامون نوآوری‌های وب۳ در راستای حمایت از مصرف‌کننده/سرمایه‌گذار و یکپارچگی بازار وجود دارد. قابل‌توجه‌ترین قوانین پیشنهادی عبارتند از: «DCCPA» در ایالات‌متحده، «MiCA» در اتحادیه اروپا، پیشنهادات «قوانین استیبل‌کوین» در سنگاپور، و طرح مجوز «ETF» کریپتو در هنگ‌کنگ.

۲. متخصصان و تنظیم‌کننده‌های وب۳ باید با یکدیگر همکاری کنند تا راه‌های جدیدی برای تکمیل خودتنظیمی با مقررات دولتی تعریف کنند.

۳. ماهیت بدون مرز فناوری‌های وب ۳ چالش‌های قضائی را به همراه دارد که مقررات فعلی هنوز به آن‌ها رسیدگی نکرده است، ازجمله مسئله مالیات بین‌المللی.

عنوان: Event Recap: Policymaking in Web3
نویسنده: Helena Rong , Sarah Hubbard
مرکز مطالعاتی: Belfercenter
تاریخ انتشار: December 16, 2022

فرصت‌ها و چالش‌های طرح کاخ سفید برای منشور حقوق هوش مصنوعی

در اکتبر ۲۰۲۲، دفتر سیاست علم و فناوری کاخ سفید (OSTP) طرحی برای منشور حقوق هوش مصنوعی (Blueprint) منتشر کرد که نقشه راه غیر الزام‌آور برای استفاده مسئولانه از هوش مصنوعی را به اشتراک گذاشت. این سند جامع پنج اصل را برای هدایت و حاکمیت توسعه و اجرای مؤثر سیستم‌های هوش مصنوعی باتوجه خاص به پیامدهای ناخواسته نقض حقوق مدنی و حقوق بشر شناسایی کرده است. درحالی‌که شناسایی و کاهش خطرات مورد نظر و ناخواسته هوش مصنوعی مدت زیادی است که به‌طور گسترده‌ای شناخته شده است، چگونگی تسهیل این شکایات توسط طرح اولیه هنوز مشخص نشده است. علاوه‌براین، سؤالاتی در خصوص اینکه آیا این سند غیرالزام‌آور باعث اقدام لازم کنگره برای اداره این فضای غیرقانونی می‌شود، مطرح شده است.

مرکز نوآوری فناوری بروکینگز در ۵ دسامبر ۲۰۲۲ میزبان گفتگو با کارشناسان OSTP، اندیشکده‌ها و سازمان‌های عدالت اجتماعی بود که در طی آن، مهمانان ضمن بحث درمورد محدودیت‌های بالقوه، جنبه‌های کلیدی طرح را بازگشایی کردند. برخی فکر می‌کردند که این آسیب‌ها خیلی گسترده تعریف شده‌اند و به طرح این پرسش پرداختند که آیا آژانس‌های فدرال منابع لازم برای پایبندی به شیوه‌ها و رویه‌های مسئول درمورد خرید، استفاده و ممیزی‌های مداوم هوش مصنوعی را دارند؟

ازنظر پیشرفت قبل و بعد از انتشار طرح اولیه، حداقل پنج آژانس فدرال دستورالعمل‌هایی را برای استفاده مسئولانه خود از سیستم‌های خودکار اتخاذ کرده‌اند. اصول اخلاقی وزارت دفاع (DOD) برای هوش مصنوعی و برنامه اقدام هوش مصنوعی آژانس توسعه بین‌المللی ایالات‌متحده، هر دو دستورالعمل‌هایی را درخصوص استفاده دولت از هوش مصنوعی اجرا کرده‌اند. کمیسیون فرصت‌های شغلی برابر (EEOC) همچنین ابتکار عمل هوش مصنوعی و عدالت الگوریتمی خود را در همکاری با وزارت کار راه‌اندازی کرده است.

عنوان	Opportunities and blind spots in the White House's blueprint for an AI Bill of Rights
نویسنده	Nicol Turner Lee , Jack Malamud
مرکز مطالعاتی	Brookings
تاریخ انتشار	December 19, 2022

تأثیر سوابق داده افراد بر ارتقای موقعیت شغلی

این گزارش بررسی می‌کند که چگونه اعتبار دیجیتال و سوابق یادگیری و اشتغال (LERs) راه‌های دسترسی افراد به آموزش و فرصت‌های شغلی را در سراسر جهان شکل می‌دهند. اگرچه این فناوری‌های جدید ممکن است فرصت‌ها را برای بسیاری از یادگیرندگان و کارگران گسترش دهند، اما خطر ترک بسیاری از جوامع و افراد از شغل خود را نیز در پی دارند.

این گزارش ابتدا روندها و بحث‌های اصلی را درمورد چگونگی ایجاد فرصت‌ها و چالش‌های جدید فناوری‌های آموزشی برای دستیابی به اهداف توسعه پایدار سازمان ملل متحد تبیین می‌کند. علی‌رغم علاقه روزافزون و رشد سریع در این اکوسیستم‌ها، پذیرش گسترده اعتبارنامه‌های دیجیتال هنوز در مراحل اولیه است. نهادهای اساسی، چارچوب‌های نظارتی و سیاست‌های موردنیاز برای اداره فناوری به‌طورکلی و به‌طور خاص برای کمک به مردم برای درک گستردگی روزافزون گزینه‌های یادگیری دیجیتال و استخدام بسیار نوپا هستند. بسیاری از ابتکارات، مانند تلاش برای دیجیتالی کردن مدارک و سوابق یادگیری، مبارزه با آگاهی کم، کمبود ظرفیت فنی، خطرات امنیت داده‌ها و درک محدود از نحوه رویکرد دیجیتالی شدن از این نمونه‌ها هستند. ما استدلال می‌کنیم که فرآیند تدریجی پذیرش، فرصتی برای ذی‌نفعان کلیدی مانند دولت‌ها، ارائه‌دهندگان آموزش عالی و کارفرمایان فراهم می‌کند تا سیستم‌ها و فناوری‌های زیربنایی خود را با هدف پیشبرد دسترسی اخلاقی و عادلانه به آموزش و یادگیری مادام‌العمر هماهنگ کنند.

عنوان	Going digital: How learning and employment records shape access to quality education and jobs
نویسنده	Annelies Goger , Allyson Parco , Rohan Carter-Rau , Jessa Henderson , Kazumi Homma , Ani Meliksetyan, Natalie Milman
مرکز مطالعاتی	Brookings
تاریخ انتشار	December 8, 2022

چگونگی تبلیغات روسیه در آمریکای لاتین و تأثیر پلتفرم بر آن

با گسترش جنگ کرملین علیه اوکراین، رسانه‌های دولتی روسیه و حساب‌های دیپلماتیک آنلاین تلاشی هماهنگ برای گسترش تبلیغاتی را آغاز کردند که هدف آن توجیه یا منحرف کردن سرزنش خشونت است. آن‌ها به پخش این تبلیغات در سراسر جهان، ازجمله در آمریکای لاتین ادامه می‌دهند. در منطقه‌ای که هم شرکای آمریکایی و هم دوستان مسکو را در خود جای داده است، به نظر می‌رسد افکار عمومی درباره این درگیری مورد توجه قرار گرفته است.

تجزیه و تحلیل محتوای مورد حمایت دولت روسیه در توییتر و فیس‌بوک برای مخاطبان در آمریکای لاتین نشان می‌دهد که بلافاصله پس از حمله روسیه به اوکراین، رسانه‌های دولتی روسیه و حساب‌های دیپلماتیک تلاشی هماهنگ برای ارسال پیام‌های خود درباره درگیری به مخاطبان در آمریکای لاتین آغاز کردند. باتوجه‌به داده‌های جمع‌آوری‌شده برای این مقاله، نسبت تمام پست‌های مربوط به موضوعات متمرکز بر اوکراین توسط این حساب‌ها سه برابر شد و درگیری با پست‌های مربوط به اوکراین - در قالب لایک، نظر، اشتراک‌گذاری و سایر واکنش‌ها - بیش از ۴۰۰ درصد افزایش یافت. تبلیغات کرملین به دنبال توجیه تهاجم با ادعای وجود یک تهدید جدی بود؛ مسکو استدلال کرد که دولت اوکراین در حال نسل‌کشی علیه مردم روسی‌زبان در بخش شرقی این کشور است. با ادامه جنگ، تبلیغات کرملین نیز به دنبال این بود که سرزنش کمبود غذا و سوخت جهانی را این‌گونه توجیه کند که کمبودها نتیجه تحریم‌های غرب علیه روسیه است.

کرملین از اینفلوئنسرها - عمدتاً روزنامه‌نگاران مستقل اسپانیایی‌زبان - برای تقویت قدرت پیام خود استفاده می‌کند. از ۱۵ حساب برتر، ۷ مورد از روزنامه‌نگاران مستقل اسپانیایی زبان هستند که به رسانه‌های دولتی روسیه وابسته نیستند.

باتوجه به گستردگی تعامل با محتوای مورد حمایت روسیه در منطقه و پیامدهای آن برای منافع ایالات‌متحده، واشنگتن باید اقدامات مشخصی را برای اطمینان از آمادگی برای مقابله با این چالش انجام دهد. برای شروع، باید منابع دیپلماسی عمومی بیشتری را به آمریکای لاتین اختصاص دهد. این امر می‌تواند مستلزم تجهیز وزارت امور خارجه ایالات‌متحده برای ردیابی بهتر فعالیت‌های تبلیغاتی روسیه در آن‌جا، سرمایه‌گذاری در آژانس ایالات‌متحده برای رسانه‌های جهانی با هدف مخاطبان آمریکای لاتین و حمایت از تحقیقات درمورد موضوعات مرتبط باشد. در سطح تاکتیکی، واشنگتن باید بر تاکتیک‌های اطلاعات نادرست کرملین و فعالیت‌های مداخله‌ای در منطقه تمرکز کند. درنهایت، باتوجه به تأثیری که به نظر می‌رسد سیاست‌های پلتفرم بر گسترش محتوای مورد حمایت دولت روسیه دارند، شفافیت بیشتر پلتفرم‌ها درباره ماهیت سیاست‌ها به سیاست‌گذاران کمک می‌کند مسیری رو به جلو ترسیم کنند.

عنوان Working the Western Hemisphere, How Russia spreads propaganda about Ukraine in Latin America and the impact of platform responses
نویسنده Jessica Brandt , Valerie Wirtschafter
مرکز مطالعاتی Brookings
تاریخ انتشار December 18, 2022

ایمن‌سازی 5G

از شهرهای هوشمند، تا خودروهای هوشمند و کارخانه‌های هوشمند، آینده براساس ریزتراشه‌های همه‌جانبه متصل به شبکه‌های بی‌سیم ساخته خواهد شد. فناوری نسل پنجم (5G) نوید ارائه زیرساخت‌های بی‌سیم با سرعت بالا و تأخیر کم را برای عصر «هوشمند» می‌دهد. بااین‌حال، حرکت از وعده به واقعیت مستلزم ایمن بودن آن شبکه‌هاست.

معرفی شبکه‌های 5G، هم پاسخی به موج عظیم دیجیتالی شدن است که اقتصاد را فرا گرفته و هم محرکی برای گسترش بیشتر آن است. براساس برخی برآوردها، نیمی از کل ترافیک داده در سراسر جهان طی پنج سال آینده نه توسط افراد، بلکه توسط دستگاه‌های رایانه‌ای که نیازی به دخالت انسانی ندارند، ایجاد خواهد شد.

شبکه‌های بی‌سیم نسل پنجم قابلیت‌ها و خدمات جدید شگفت‌انگیز و مهمی را ارائه خواهند داد. بااین‌حال، 5G همچنین چالش‌های جدید امنیت سایبری را به همراه دارد. ایمن‌سازی شبکه‌هایی که از اجزای بالقوه ناامن استفاده می‌کنند در شرایطی که در دنیایی ذاتاً ناامن کار می‌کنند یک چالش جدید است. این مشکلی است که با چگونگی رشد تصاعدی در ترافیک داده‌ها، کارآمدی نظارت بر امنیت سایبری مبتنی بر ترافیک سنتی را به خطر می‌اندازد.

هدف این مقاله انتقاد از مهندسی شگفت‌انگیز تولید 5G نیست. بلکه توجه به این امر است که چگونه این تصمیم‌ها، با معرفی یک معماری شبکه جدید، در پرداختن به خطرات امنیت سایبری قابل‌اجتناب و همچنین معرفی نگرانی‌های جدید امنیت سایبری کوتاهی کرده‌اند؛ و نشان دادن این‌که چگونه می‌توان این نگرانی‌ها را با ترکیبی از نظارت چابک، تمرکز شرکتی و بودجه دولتی کاهش داد.

عنوان	5G is smart, now let's make it secure
نویسنده	Tom Wheeler, David Simpson
مرکز مطالعاتی	Brookings
تاریخ انتشار	December 12, 2022

نحوه اصلاح قانون داده پیشنهادی اتحادیه اروپا

هدف پیش‌نویس قانون داده اتحادیه اروپا که توسط کمیسیون اروپا در فوریه ۲۰۲۲ پیشنهاد شد، پر کردن شکاف بزرگ در مقررات مربوط به داده‌ها است؛ مقابله با وضعیتی که در آن سازندگان ماشین‌ها را به‌گونه‌ای طراحی می‌کنند تا به داده‌های تولیدی آن‌ها، دسترسی انحصاری داشته و در ادامه خدمات مبتنی‌بر داده تولیدی ماشین را باز هم به‌صورت انحصاری به کاربران می‌فروشند. این امر رقابت در بازارهای خدمات مبتنی‌بر داده تولیدی ماشین را مخدوش می‌کند.

برای نمونه، یک کشاورز ممکن است بخواهد به داده‌های مزرعه جمع‌آوری‌شده توسط تراکتور خود دسترسی داشته باشد و آن را با سایر ماشین‌های مورد استفاده در کنار تراکتور یا با ارائه‌دهندگان خدمات کشاورزی به اشتراک بگذارد. این کار می‌تواند او را قادر سازد تا توصیه‌های کشاورزی بهتری دریافت کرده یا استفاده از ماشین‌های بذرپاشی و سمپاشی را با دقت بالاتری تنظیم کند. اما درحال‌حاضر، تولیدکنندگان ماشین‌های کشاورزی می‌توانند از دسترسی و انتقال داده‌ها جلوگیری کرده و کشاورزان را مجبور به استفاده از خدمات کشاورزی مرتبط با خود کنند.

بنابراین کنترل داده‌های انحصاری توسط تولیدکنندگان محصول به مالکیت واقعی داده‌ها خلاصه می‌شود. اما صدور چنین مجوزهای حقوقی برای مالکیت انحصاری به یک طرف، ادعاهای سایر تولیدکنندگان داده را رد کرده و از نظر اقتصادی ناکارآمد به‌شمار می‌آید، زیرا داده‌ها غیررقیب هستند و می‌توان از آن برای اهداف تولیدی توسط چندین طرف به‌طور همزمان استفاده کرد. تمرکز قانون داده بر حقوق دسترسی گامی خوشایند، قاطع و به دور از مالکیت انحصاری داده است. این قانون، در صورت تصویب توسط پارلمان اروپا و شورای اتحادیه اروپا، تکمیل‌کننده سایر قوانین داده، ازجمله مقررات عمومی حفاظت از داده اتحادیه اروپا (GDPR) خواهد بود که به افراد اجازه دسترسی به داده‌های شخصی خود را می‌دهد، اما درخصوص دسترسی کسب‌وکارها به صنعت خود چیزی نمی‌گوید..

عنوان	How to fix the European Union's proposed Data Act
نویسنده	Bertin Martens
مرکز مطالعاتی	Bruegel
تاریخ انتشار	December 14, 2022

عملیات سایبری روسیه در زمان جنگ در اوکراین: تأثیرات و پیامدهای نظامی

این مقاله بخشی از مجموعه مقاله اندیشکده کارنگی با عنوان «درگیری سایبری در جنگ روسیه و اوکراین» است؛ پروژه‌ای برای درک بهتر عناصر سایبری جنگ روسیه و اوکراین. کارشناسان کارنگی هرکدام یک بعد منحصربه‌فرد از درگیری سایبری را بررسی می‌کنند؛ نیک بیکرافت «Nick Beecroft» درمورد کمک بین‌المللی به دفاع سایبری اوکراین، گاوین وایلد «Gavin Wilde» درباره انتظارات برآورده‌نشده روسیه و جان بیتمن «Jon Bateman» درمورد تأثیر نظامی کلی عملیات سایبری روسیه.

این مقاله به بررسی اثربخشی نظامی عملیات سایبری روسیه در زمان جنگ در اوکراین می‌پردازد، دلایلی که چرا این عملیات‌ها تأثیر استراتژیک بیشتری نداشته‌اند، و درس‌های قابل‌استفاده برای تلاش‌های سایبری نظامی دیگر کشورها. هدف اصلی این مقاله کمک به پل زدن بین تجزیه و تحلیل نظامی سایبری خاص و عام از جنگ روسیه و اوکراین است. بیشتر تحلیل‌های عملیات سایبری روسیه در اوکراین توسط متخصصان سایبری که برای حوزه خودشان می‌نویسند، با ادغام محدود منابع و مفاهیم نظامی غیرسایبری تهیه شده است. برعکس، گزارش‌های پیش‌رو از جنگ به‌عنوان یک کل، عملاً هیچ اشاره‌ای به عملیات سایبری ندارد. این مقاله، عملیات سایبری روسیه در اوکراین را در چارچوب بزرگ‌تر اهداف نظامی، کمپین‌ها و فعالیت‌های جنبشی مسکو قرار می‌دهد. نکات کلیدی آن عبارتند از:

۱. حملات سایبری روسیه ممکن است در تهاجم اولیه مسکو نقش به‌سزایی داشته باشد، اما از آن زمان تاکنون خسارت ناچیزی به اهداف اوکراینی وارد کرده است.
۲. جمع‌آوری اطلاعات احتمالاً محور اصلی عملیات سایبری روسیه در زمان جنگ در اوکراین بوده است، اما این نیز سود نظامی کمی به همراه داشته است.
۳. درحالی‌که بسیاری از عوامل اثربخشی سایبری مسکو را محدود کرده‌اند، شاید مهم‌ترین آن‌ها ظرفیت سایبری ناکافی روسیه، ضعف در نهادهای غیرسایبری روسیه و تلاش‌های دفاعی استثنایی اوکراین و شرکای آن باشد.
۴. با ادامه جنگ، مجموعه اطلاعاتی روسیه احتمالاً بزرگ‌ترین خطر سایبری مداوم برای اوکراین است.
۵. سرمایه‌گذاری‌های کشورها در جمع‌آوری اطلاعات سایبری باید با تلاش‌های اختصاصی یکسانی برای ارتقای تحلیل اطلاعاتی، برنامه‌ریزی نظامی و تصمیم‌گیری استراتژیک همراه باشد.
۶. مدافعان سایبری باید از جنگ اوکراین به‌عنوان یک نقطه مرجع برای بررسی مجدد و اصلاح مفروضات قبلی درمورد جنگ‌های خاصی که ممکن است پیش بیاید، استفاده کنند.

عنوان	Russia's Wartime Cyber Operations in Ukraine: Military Impacts, Influences, and Implications
نویسنده	Jon Bateman
مرکز مطالعاتی	Carnegie
تاریخ انتشار	December 16, 2022

عملیات سایبری در اوکراین: انتظارات برآورده‌نشده روسیه

این گزارش کارنگی، با مروری بر نوشته‌های دانشگاهی و روزنامه‌نگاری‌هایی که در سه دهه اخیر نظریه‌پردازی ارتش روسیه درمورد موضوعات مرتبط با سایبری را پوشش داده، سه فرضیه را مطرح می‌کند که ممکن است عدم‌تطابق بین انتظارات بسیاری از ناظران غربی و تأثیر گزارش‌شده عملیات سایبری روسیه در سال ۲۰۲۲ را توضیح دهد. تهاجم به اوکراین با بررسی جنبه‌های منحصربه‌فرد و اغلب نادیده گرفته‌شده مفهوم‌سازی مسکو از «سایبر» بود. این مقاله همچنین پایه‌ای برای ارزیابی بهتر عملکرد سایبری روسیه در اوکراین در بازه زمانی اوایل سال ۲۰۲۲، همراه با درک دقیق‌تری از قابلیت‌ها و توانایی‌های آن ارائه می‌دهد. برخی از محورهای کلیدی این گزارش عبارت است از:

۱. نیروهای عملیات اطلاعاتی روسیه (مشابه با فرماندهی سایبری نظامی غربی) در مراحل ابتدایی خود باقی مانده و بیشتر برای ضدتبلیغات بهینه شده است تا برای عملیات سایبری تهاجمی. درعین‌حال، ساختار فرماندهی عملیاتی در عملیات سایبری تهاجمی همچنان مبهم است و احتمالاً بیشتر ماهیت سیاسی دارد تا نظامی.

۲. برترین ظرفیت‌های سایبری تهاجمی روسیه در سازمان‌های متمرکز بر اطلاعات و براندازی قرار دارند تا اینکه در حوزه جنگ‌های تسلیحاتی ترکیبی فعالیت کنند.

۳. تهاجم مخفیانه و ضعیف مسکو در فوریه ۲۰۲۲ مانع از عملکرد مطلوب در دوره اولیه جنگ شد که به‌ویژه در تفکر روسیه درمورد اثربخشی در حوزه اطلاعات بسیار مهم است.

عنوان	Cyber Operations in Ukraine: Russia's Unmet Expectations
نویسنده	Gavin Wilde
مرکز مطالعاتی	Carnegie
تاریخ انتشار	December 12, 2022

استفاده از هوش مصنوعی برای تأمین مالی پایدار

تحولات در هوش مصنوعی و یادگیری ماشین منجر به شکل‌گیری نوع جدیدی از داده‌های ESG شده است که لزوماً به اطلاعات ارائه‌شده توسط شرکت‌ها متکی نیست. نویسندگان این مقاله استفاده از هوش مصنوعی را در زمینه ESG مرور می‌کنند؛

۱. تجزیه و تحلیل متنی برای اندازه‌گیری رویدادهای محیطی، اجتماعی و حاکمیتی شرکت‌ها یا تأیید اعتبار تعهدات ملموس شرکت‌ها، داده‌های ماهواره و حسگر برای تجزیه‌وتحلیل محیطی شرکت‌ها.
۲. تأثیر یا برآورد مخاطرات یادگیری ماشینی برای پر کردن داده‌های گمشده شرکت.

این مقاله سپس چالش‌های بالقوه را ازنظر شفافیت، خطرات دستکاری و هزینه‌های مرتبط با این داده‌ها و ابزارهای جدید مورد بحث قرار می‌دهد.

عنوان	Artificial Intelligence for Sustainable Finance
نویسنده	Marie Briere, Matthieu Keip, Tegwen Le Berthe
مرکز مطالعاتی	Ceps
تاریخ انتشار	December 15, 2022

تأثیر نوسانات ارزهای دیجیتال بر کشورها

در سال‌های اخیر، چندین کشور شروع به پذیرش بیت‌کوین به‌عنوان نوعی پول قانونی نموده‌اند و از پتانسیل آن برای متحول کردن اقتصاد خود استقبال کرده‌اند. اما در سال ۲۰۲۲، بازارهای ارزهای دیجیتال سقوط کردند. بعد از زمانی که در نوامبر ۲۰۲۱ به بیش از ۶۸۰۰۰ دلار رسید، قیمت بیت‌کوین به زیر ۱۷۰۰۰ دلار کاهش یافت. این نوسانات، که با فروپاشی صرافی ارزهای دیجیتال FTX و سایر سرمایه‌گذاری‌های رمزنگاری محقق شد، بررسی‌های جدیدی را برای کشورهایی که دارایی‌های دیجیتال را به رسمیت پذیرفته‌اند، ضروری کرده است.

کدام کشورها ارزهای رمزنگاری‌شده را به‌عنوان ارز قانونی پذیرفته‌اند؟

دو کشور السالوادور و جمهوری آفریقای مرکزی (CAR) به‌طور رسمی بیت‌کوین را به‌جای پول قانونی پذیرفته‌اند. در همین حال، کشورهای دیگر تمایل خود را برای پذیرش ارزهای دیجیتال مختلف به‌جای ارز قانونی نشان داده‌اند. در نوامبر ۲۰۲۲، نخست‌وزیر کشور سَنت کیتس و نویس «Saint Kitts and Nevis» اظهار کرد که بیت‌کوین کَش (یک ارز دیجیتال جداگانه اما مرتبط) می‌تواند در سال ۲۰۲۳ به ارز قانونی در کشورش تبدیل شود. به شهروندان اجازه دهید مالیات‌های محلی را به بیت‌کوین و دو ارز دیجیتال دیگر بپردازند. تعداد انگشت‌شماری از کشورهای دیگر، مانند بلاروس و سنگاپور، مالکیت ارزهای دیجیتال توسط افراد خصوصی را ازطریق مشوق‌های مالیاتی تسهیل کرده‌اند. در همین راستا این مقاله در پی پاسخ به سؤالات زیر است:

۱. چرا کشورها بیت‌کوین را ارز رسمی خود کرده‌اند؟
۲. انتقادات به ارز دیجیتال به‌جای پول قانونی چیست؟
۳. آیا مقررات بیشتری در انتظار ارزهای دیجیتال است؟
۴. دولت‌ها چه ریسک‌هایی را باید در قبال پذیرش رمزارزها بپذیرند؟

عنوان	What Does the Cryptocurrency Decline Mean for Bitcoin Countries?
نویسنده	Noah Berman
مرکز مطالعاتی	CFR
تاریخ انتشار	December 21, 2022

گردآوری اطلاعات منبع‌باز در اوکراین

گردآوری اطلاعات منبع‌باز[۱] (Open-source intelligence یا OSINT) شاید به‌طور هم‌زمان شناخته‌شده‌ترین و ناشناخته‌ترین زمینه اطلاعاتی امروزی باشد و شامل تمام اطلاعات در دسترس عموم است که از هر منبع درمورد هر موضوعی به دست می‌آید. باتوجه به این موضوع، دامنه آن فوق‌العاده بزرگ بوده و دانش به‌دست‌آمده از آن مدت‌هاست که توسط غیرنظامیان در طول درگیری‌ها برای کمک به نیروهای خودی در نبرد استفاده می‌شود.

OSINT در طول زمان، تکامل یافته است. از سرویس اطلاعاتی برودکست خارجی در طول جنگ جهانی دوم گرفته تا فیلم‌های جغرافیایی نیروهای روسی که توسط غیرنظامیان اوکراینی در تلفن‌های همراهشان ضبط شده است، OSINT یک سنت دیرینه در حمایت غیرنظامیان از فعالیت‌های جنگی است. تهاجم روسیه به اوکراین، همراه با ماهیت به‌سرعت در حال تکامل فناوری مدرن، OSINT را در کانون توجه بی‌سابقه‌ای قرار داده است. استفاده از گردآوری اطلاعات منبع‌باز از یک تمرین عمدتاً داوطلبانه توسط افراد متخصص به یک زمینه تحقیقاتی روبه‌رشد با دفاتر دولتی که واحدهای OSINT خود را راه‌اندازی می‌کنند، تبدیل شده است.

۱. به نوعی جمع‌سپاری جمع‌آوری اطلاعاتی است که از زمان جنگ اوکراین برجسته شده است.

عنوان	Open-source intelligence in Ukraine: Asset or liability?
نویسنده	Magdalene Karalis
مرکز مطالعاتی	Chathamhouse
تاریخ انتشار	December 16, 2022

سازوکار کنترل صادرات فناوری از آمریکا

شناخت خطرات انتقال بدون محدودیت فناوری به چین، منجر به موجی از پیشنهادها برای کنترل‌های جدید صادرات در شورای تجارت و فناوری و شاید با مجموعه‌ای از کشورهای تولیدکننده نیمه‌هادی‌ها شده است. این پیشنهادها به‌موقع هستند، اما تجربه مستقیم با ایجاد سازوکار به الزامات ضروری برای تبدیل ایده‌های آرمانی به یک سازوکار واقعی اشاره می‌کند. در اینجا برخی از این الزامات آورده شده است؛

شرکای بالقوه باید با مشکل مشترکی که نیازمند اقدام جمعی است، شروع کنند. کنترل‌های صادراتی باید پس از پایان جنگ سرد اصلاح شود (برای اروپایی‌ها این به معنای کاهش کنترل‌ها و برای ایالات‌متحده به معنای حفظ آن‌هاست). حفظ سلطه فناوری ایالات‌متحده، یک هدف برای بسیاری از پیشنهادات فعلی اروپایی‌ها نیست، بلکه نگرانی‌های اروپایی‌ها را بیشتر کرده و احتمالاً ایده‌ای برای مشارکت وجود ندارد. بهترین مورد برای یک سازوکار جدید را می‌توان حول رفتار تجاری چین، جهت تصاحب غیرقانونی مالکیت معنوی و بسیاری از اقدامات قهری آن ایجاد کرد.

عنوان	Notes on Creating an Export Control Regime
نویسنده	James Andrew Lewis
مرکز مطالعاتی	CSIS
تاریخ انتشار	December 15, 2022

مدار پایین، ریسک بالا

رقابت برای ارائه پهنای باند از مدار پایین زمین (LEO) یکی از مهم‌ترین و مغفول‌ترین پیشرفت‌های ژئواستراتژیک در حال انجام است. سیاست‌گذاران در واشنگتن هنوز پیامدهای اقتصادی و استراتژیک منظومه‌های ماهواره‌ای مدار پایین را که نویدبخش بهبود چشم‌گیر پوشش شبکه در بخش‌های کم‌تر توسعه‌یافته بوده و امکان آنلاین کردن بخش‌های بیشتری از جهان را دارد، در نظر نگرفته‌اند. علاوه بر به دست آوردن فواید تجاری گسترده، کشورهای دارای ارائه‌دهندگان پیشرو پهن باند LEO می‌توانند از انعطاف‌پذیری بیشتر در ارتباطات، دقت در خدمات موقعیت‌یابی و حتی افزایش قابلیت هشدار اولیه برخوردار شوند.

گروهی از شرکت‌ها، عمدتاً از ایالات‌متحده و اروپا، در لبه توسعه این تلاش‌ها هستند. اما چین برنامه‌های خاصی برای توسعه شبکه پهن‌باند LEO داشته و با تخصیص منابع مالی عمیق دولتی این سیاست‌ها را در طرح کمربندی جاده ابریشم خود پیگیری می‌کند. با تشدید رقابت شبکه پهن‌باند LEO، سیاست‌گذاران برای پیشبرد منافع ایالات‌متحده به راهنمای قابل دسترس برای این پیشرفت‌ها و توصیه‌ها نیاز دارند.

عنوان	Low Orbit, High Stakes
نویسنده	Makena Young, Akhil Thadani
مرکز مطالعاتی	CSIS
تاریخ انتشار	December 14, 2022

تحلیلی درخصوص پیش‌نویس قانون مقاومت سایبری

مرکز نوآوری داده، تحلیل خود را درمورد درخواست شواهد در قانون مقاومت سایبری «Draft Cyber Resilience Act» ارائه کرده است. این مرکز قبلاً نظر خود را درباره نقشه راه قانون مقاومت سایبری مطرح نموده و از نزدیک پیشرفت آن را دنبال می‌کرد. این مرکز مایل است از اتحادیه اروپا (EU) به دلیل تمرکز بر تهدید فزاینده حوادث امنیت سایبری که پیش‌بینی می‌شود تا سال ۲۰۲۵، ۱۰٫۵ تریلیون دلار هزینه داشته باشد، قدردانی کند. قانون مقاومت سایبری گامی مهم در جهت‌یابی درست است.

متأسفانه، پیش‌نویس قانون مقاومت سایبری بسیار گسترده بوده و نیاز به تعاریف واضح‌تری دارد. تله‌های اساسی این قانون باعث می‌شود تا کسب‌وکارها زیر بار انطباق رفته و در نتیجه راه‌های نوآورانه‌ای مانند نرم‌افزار منبع‌باز را تضعیف کنند. به‌شکل خاص، کمیسیون اروپا باید اقدامات زیر را برای رسیدگی به مشکلات موجود در قانون مقاومت سایبری انجام دهد؛

۱. تعهدات گزارش‌دهی در قانون مقاومت سایبری برای کسب‌وکارها ساده شود.
۲. شفاف‌سازی دسته‌بندی محصولات و مشخصات فنی در قانون مقاومت سایبری، ضمن ایجاد دستورالعمل‌های انعطاف‌پذیر برای اجرای مقررات درمورد فناوری‌های آینده.
۳. تمرکز بر مداخله نظارتی بخشی، اطمینان از اینکه قوانین امنیت سایبری انعطاف‌پذیر است و می‌تواند با پیشرفت‌های فناوری تکامل یابد و برای نیازهای صنعت خاص محدود شود.
۴. تعریف نرم‌افزار متن‌باز روشن شود و به‌وضوح از شمول قانون مقاومت سایبری مستثنی گردد.
۵. سؤالات مربوط به خدمات رایانش ابری روشن شود تا اطمینان حاصل گردد که کسب‌وکارها نیاز به رعایت آن‌ها دارند یا خیر.

عنوان	Feedback to the European Commission on the Draft Cyber Resilience Act
نویسنده	Kir Nuthi
مرکز مطالعاتی	ITIF
تاریخ انتشار	December 15, 2022

مدیریت دیجیتال کره جنوبی

دیجیتالی شدن برای اقتصاد و جامعه بسیار مهم است و همه‌گیری کرونا این روند را دوباره تسریع کرده و به‌وضوح نشان داده است که استراتژی‌های دولت مرکزی تا چه حد از این توانایی برخوردارند. پذیرش فناوری‌های دیجیتال نه‌تنها می‌تواند فرایندهای داخلی و شیوه‌های دولتی را متحول کند، بلکه به‌طور قابل‌توجهی به طراحی و ارائه خدمات عمومی کمک می‌کند. کیفیت و قابلیت اطمینان‌بخشی خدمات عمومی نقش کلیدی در افزایش شفافیت، شمول و پایداری دارد.

علی‌رغم تلاش‌های فراوان برای پیاده‌سازی سیستم دولت الکترونیک، آلمان در مقایسه با سایر کشورهای OECD در شاخص دولت دیجیتال (2019) (DGI) عملکردی کمتر از میانگین دارد. ازسوی دیگر، کره جنوبی همیشه در صدر DGI قرار داشته و در تمام ابعاد بررسی‌شده با عملکردی بالاتر از حد متوسط می‌درخشد. کره جنوبی سریع‌تر از هر کشور دیگری در جهان یک دولت عمل‌گرا، شفاف و کارآمد ساخته است. بنابراین به نظر می‌رسد پرداختن به ساختارها و فرآیندهای پشت‌پرده اجرای موفقیت‌آمیز سیستم دولت الکترونیک در کره جنوبی ضروری است.

سیستم دولت الکترونیک کره جنوبی بر سه جنبه اصلی تمرکز دارد: G4C (دولت برای شهروندان)، G4B (دولت برای تجارت) و G2G (دولت به دولت). این متن در درجه اول به دو نمونه از بعد G4C اشاره کرده است. از یک‌سو به طراحی و اجرای خدمات دیجیتال شهروندی و ازسوی دیگر به مشارکت شهروندان در زمینه دولت الکترونیک می‌پردازد. نحوه طراحی و در دسترس قرار دادن ساختارهای خدماتی توسط یک دولت تأثیر عمده‌ای بر روابط و رضایت شهروندان از آن دارد. اعتماد به شایستگی‌های یک دولت را می‌توان به‌شکل پایدار ازطریق خدمات و قالب‌های ارتباطی شهروندان دیجیتالی که به‌راحتی در دسترس هستند، تقویت کرد. دیجیتالی شدن خدمات شهروندان نه‌تنها مزایایی را برای شهروندان به ارمغان می‌آورد. بلکه کارمندان اداری نیز از این طریق منتفع شده و کارهای روزمره برایشان راحت می‌شود.

عنوان Digitale Verwaltung in Korea–mit gutem Beispiel voran
نویسنده Eva Antonia Steding
مرکزمطالعاتی KAS

حکمرانی فناوری طالبان

بیش از یک سال از انتشار تصاویر هولناکی از خروج نافرجام آمریکا از افغانستان می‌گذرد. داستان کابل و مردم افغانستان، جنگ در اوکراین، ظهور چین، و ادغام دیگر نقاط جهش ژئوپلیتیک جهانی تشدید شده است.

طالبان به تلاش‌های خود برای تحکیم یک نظام سیاسی «جدید» تحت حکومت موقت خود ادامه می‌دهد تا قدرت آینده خود را بر کشور تقویت کند. اهداف اصلی استراتژی طالبان کنترل روایت‌ها و بکارگیری استراتژی رسانه‌ای قوی است. استراتژی رسانه‌ای طالبان به دو بخش اصلی تقسیم می‌شود: اول، روایتی که متوجه غرب و جامعه بین‌المللی است. دوم، روایت برای مخاطبان داخلی. در رسانه‌های اصلی خارج از افغانستان، ما فقط در معرض روایت اول‌شخص هستیم. استراتژی رسانه‌ای معطوف به افغان‌ها تا حد زیادی در گفتمان بین‌المللی غایب است.

وضعیت فعلی طالبان معماهای جالبی را هم برای نهادهای امنیتی و هم برای شرکت‌های فناوری ایجاد می‌کند. این مقاله به دنبال بررسی این موضوع است که آیا طالبان توسط پلتفرم‌های رسانه‌های اجتماعی باید به‌عنوان یک بازیگر دولتی یا غیردولتی در نظر گرفته شود یا خیر.

(*)

عنوان: How the Taliban is Building New Grey Areas for Global Tech to Address
نویسنده: kabir Taneja
مرکز مطالعاتی: ORFonline
تاریخ انتشار: December 21, 2022

نگرانی درباره لایحه مقررات فناوری هند

در آوریل ۲۰۲۲، وزارت علوم و فناوری (MST) هند پیش‌نویس لایحه مقررات فناوری DNA (استفاده و کاربرد) را منتشر کرد. با این اطلاعیه، MST اعلام کرد که بیش از ۲۰۰۰۰ افسر تحقیقات، افسران دادستان و متخصصان پزشکی را برای جمع‌آوری شواهد پزشکی قانونی در موارد تجاوز جنسی با استفاده از کیت‌های استاندارد آموزش می‌دهد.

لایحه فناوری DNA، در پیش‌نویس خود، راه‌اندازی بانک‌های داده‌های DNA در سراسر کشور و آزمایشگاه‌های DNA برای آزمایش و ذخیره پروفایل‌های DNA و استفاده از آن‌ها برای حل پرونده جرایم را (در درجه اول تجاوز جنسی) به‌عنوان هدف خود اعلام کرده است. قبل از این پیش‌نویس، هیچ قانون خاصی در هند وجود نداشت که دستورالعمل‌های مربوط به جمع‌آوری، ذخیره و استفاده از DNA در اجرای قانون را مشخص کند. بااین‌حال، مستندات DNA ذیل بخش ۴۵ قانون ۱۸۷۲ و تحت عنوان «شواهد علمی» پوشش داده شده است.

این لایحه، درحالی‌که تلاشی نجیبانه برای رسیدگی به شکاف موجود در تنظیم استفاده از شواهد نمونه بیولوژیکی است، نگرانی‌هایی را درمورد سوگیری در قانون و فقدان حریم خصوصی و حیثیت افراد ایجاد می‌کند. سیاست‌گذاران و مقامات مربوطه باید قبل از اینکه چنین قوانینی به سایر حوزه‌های اجرای قانون گسترش یابد، به این مسائل بپردازند.

عنوان	DNA Technology Regulation Bill: Concerns on data privacy, dependence, and bias
نویسنده	Shravishtha Ajaykumar
مرکز مطالعاتی	ORFonline
تاریخ انتشار	December 20, 2022

ابهامات پیش‌نویس لایحه حفاظت از داده‌های شخصی دیجیتال ۲۰۲۲ هند

در ۱۸ نوامبر، وزارت الکترونیک و فناوری اطلاعات هند (MeitY) پیش‌نویس لایحه حفاظت از داده‌های شخصی دیجیتال ۲۰۲۲ (DPDPB ۲۰۲۲) را ارائه کرد. این پیش‌نویس که از ۹۰ ماده تشکیل شده است، با ۳۰ ماده مختصرتر از لوایح قبلی خود، برخی تعاریف و خطوط کلی را شامل نمی‌شود.

برای مثال یکی از این جنبه‌ها، ابهام در تعریف مفهوم رضایت است. این بخش به این موضوع می‌پردازد که چگونه حتی اگر رضایت صریح از طرف اصلی داده‌ها دریافت نشود، امکان نگهداری داده‌های شخصی در پایگاه داده‌های امانت‌دار وجود دارد. مثال ارائه‌شده در اینجا مربوط به نگهداری داده‌های بیومتریک کارکنانی است که با استفاده از سیستم‌های بیومتری به محل کار وارد و از آن خارج می‌شوند. فرض بر این است که سازمان‌های میزبان داده مورد بحث در این لایحه پاسخگو نیستند و نیازی به حذف اطلاعات ذکرشده ندارند، زیرا جمع‌آوری این داده‌ها برای رسیدگی‌های شغلی ضروری است. این مثال که در لایحه ارائه شده است و بسیاری از موارد دیگر، جرقه‌ای برای بحث درباره لزوم روشن شدن بسیاری از مفاهیم ذکرشده در این لایحه را ایجاد می‌کند.

عنوان	The ambiguities in India's attempt at data protection
نویسنده	Shravishtha Ajaykumar
مرکز مطالعاتی	ORFonline
تاریخ انتشار	December 17, 2022

حق برآگاهی برای حفاظت از داده‌های شخصی

وزارت الکترونیک و فناوری اطلاعات (MeitY) در ۱۸ نوامبر پیش‌نویس لایحه حفاظت از داده‌های شخصی دیجیتال ۲۰۲۲ را منتشر کرد. این لایحه حقوق زیادی را به مدیران کنترل داده‌های کاربران اعطا می‌کند، مانند حق تصحیح و پاک کردن داده‌های شخصی (بخش ۱۳)، حق رسیدگی به شکایات (بخش ۱۴) و حق بر نمایندگی (بخش ۱۵) و از همه مهم‌تر، حق بر آگاهی (بخش ۱۲) درمورد داده‌های شخصی. بخش ۱۲ به مدیران داده این اختیار را می‌دهد که خلاصه‌ای از داده‌های پردازش‌شده توسط متولیان داده یا نهادهایی که هدف و ابزار پردازش داده‌ها را تعیین می‌کنند، دریافت نمایند (به همراه جزئیات همه امانت‌داران داده که داده‌های شخصی را در اختیار داشته‌اند). این خلاصه وضعیت برای استفاده از حقوق توسط مدیر داده بسیار مهم است. به‌عنوان نمونه، هنگامی که مدیر داده خلاصه‌ای از داده‌های در حال پردازش را در اختیار داشته باشد، می‌تواند اطلاعات پردازش‌شده را تصحیح کند یا حتی شکایتی را از امانت‌دار داده ثبت نماید.

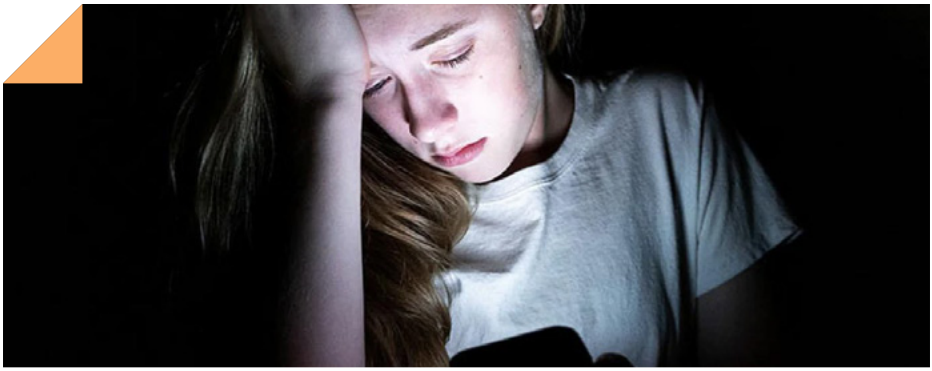
«حق بر آگاهی» موظف است نقشی محوری برای شهروندان ایفا کند تا آنان از حقوق خود استفاده کنند و وظایف خود را همان‌طور که در لایحه ذکر شده انجام دهند. به‌علاوه، این لایحه برخی وظایف را متوجه مدیران کرده است، مانند: رعایت مفاد کلیه قوانین قابل اجرا، پرهیز از ثبت شکایات بیهوده یا نادرست از امانت‌داران داده‌ها یا هیئت حفاظت از داده‌ها.

عنوان	Right to information is central to personal data protection
نویسنده	Antara Vats
مرکز مطالعاتی	ORFonline
تاریخ انتشار	December 8, 2022

آزار سایبری نوجوانان در سال ۲۰۲۲

براساس یک نظرسنجی مرکز تحقیقات پیو «Pew» که از ۱۴ آوریل تا ۴ می ۲۰۲۲ انجام شده است، نزدیک به نیمی از نوجوانان به‌ویژه دختران ایالات‌متحده مورد آزار و اذیت و سوءاستفاده آنلاین قرار می‌گیرند. تقریباً نیمی از نوجوانان ۱۳ تا ۱۷ ساله ایالات‌متحده (۴۶٪) گزارش می‌دهند که حداقل یکی از شش رفتار آزار و اذیت سایبری را تجربه کرده‌اند. شایع‌ترین رفتار گزارش‌شده در این نظرسنجی، آزار کلامی است، به‌طوری که ۳۲ درصد از نوجوانان گفته‌اند که آن‌ها را به‌صورت آنلاین یا ازطریق تماس تلفن همراه با نامی توهین‌آمیز خطاب کرده‌اند. ۲۲ درصد دیگر می‌گویند که شایعات نادرستی درباره آن‌ها به‌صورت آنلاین منتشر شده و ۱۷ درصد می‌گویند که تصاویر مستهجنی بدون اینکه درخواست کرده باشند، برایشان ارسال شده است.

حدود ۱۵ درصد از نوجوانان می‌گویند که این تجربه را داشته‌اند که فردی غیر از والدین دائماً از آن‌ها سؤالاتی همچون اینکه کجا هستند، چه کار می‌کنند یا با چه کسی هستند، پرسیده‌اند؛ درحالی‌که ۱۰ درصد از افراد می‌گویند که مورد تهدید فیزیکی قرار گرفته و ۷ درصد نوجوانان گفته‌اند که آن‌ها را تهدید کرده‌اند و تصاویر واضحی از بدن آن‌ها بدون رضایت‌شان به اشتراک گذاشته شده است و در مجموع ۲۸ درصد از نوجوانان ترکیبی از انواع مختلف آزار و اذیت سایبری را تجربه کرده‌اند.



عنوان	Teens and Cyberbullying 2022
نویسنده	Emily a. Vogels
مرکز مطالعاتی	PEW
تاریخ انتشار	December 15, 2022

تأثیر رسانه‌های اجتماعی بر مردم

بسیاری فکر می‌کنند رسانه‌های اجتماعی دستکاری و تفرقه بین مردم را آسان‌تر کرده است اما درعین‌حال معتقدند که باعث افزایش آگاهی شده است. از آن‌جایی که مردم در سراسر جهان به‌شکل فزاینده‌ای به فیس‌بوک، توییتر، واتس‌اپ و دیگر پلتفرم‌ها برای دریافت اخبار و بیان نظرات خود روی آورده‌اند، حوزه رسانه‌های اجتماعی به فضای عمومی جدیدی برای بحث و گفتگو - و اغلب بحث‌های تلخ و آزاردهنده در ارتباط با مسائل سیاسی و اجتماعی تبدیل شده است. در ذهن بسیاری از تحلیل‌گران، رسانه‌های اجتماعی یکی از دلایل اصلی کاهش دموکراسی در سراسر جهان است.

بااین‌حال، همان‌طور که یک نظرسنجی جدید مرکز تحقیقات پیو از ۱۹ اقتصاد پیشرفته نشان می‌دهد، شهروندان عادی بیشتر بر این باورند که رسانه‌های اجتماعی واقعاً تأثیر مثبتی بر دموکراسی داشته است. در سراسر کشورهای مورد نظرسنجی، ۵۷ درصد می‌گویند که رسانه‌های اجتماعی تأثیر مثبتی روی دموکراسی آن‌ها و ۳۵ درصد گفته‌اند که تأثیر منفی داشته است.

با وجود این، نتایج این نظرسنجی در آمریکا بسیار متفاوت از سایر کشورهاست. فقط ۳۴٪ از بزرگسالان آمریکایی فکر می‌کنند رسانه‌های اجتماعی برای دموکراسی خوب بوده است. درحالی‌که ۶۴٪ می‌گویند تأثیر بدی داشته است به‌طوری‌که بخش بیشتری از آمریکایی‌ها رسانه‌های اجتماعی را تفرقه‌افکن می‌دانند.

حتی در کشورهایی که ارزیابی‌ها از تأثیر رسانه‌های اجتماعی تا حد زیادی مثبت است، اکثر آن‌ها بر این باورند که تأثیرات مخربی داشته است؛ به‌ویژه، منجر به دستکاری و تفرقه در جوامع شده است. ۸۴ درصد از ۱۹ کشور موردبررسی، معتقدند دسترسی به اینترنت و رسانه‌های اجتماعی باعث شده است افراد با اطلاعات نادرست و شایعات مواجه شوند. تحلیل اخیر همین نظرسنجی نشان می‌دهد که ۷۰ درصد از ۱۹ کشور، انتشار اطلاعات نادرست آنلاین را یک تهدید بزرگ می‌دانند.

عنوان: Social Media Seen as Mostly Good for Democracy Across Many Nations, But U.S. is a Major Outlier

نویسنده: Richard Wike, Laura Silver, Janell Fetterolf, Christine Huang, Sarah Austin, Laura Clancy Sneha Gubbala

مرکز مطالعاتی: PEW

تاریخ انتشار: December 6, 2022

کدام لوایح حزبی به امنیت سایبری آسیب می‌زند؟

کنگره یک دوره سه‌ساله خیره‌کننده در توسعه و تصویب قوانین امنیت سایبری داشته است که هم از زیرساخت‌های حیاتی ملی آمریکا محافظت می‌کند و هم به شبکه‌های فدرال امنیت می‌دهد. بر مبنای دوحزبی و دو مجلسی، صدها ماده برای حفاظت از امنیت ملی، بهره‌وری اقتصادی و سلامت و ایمنی عمومی به قانون تبدیل شده است. بااین‌حال، لایحه «کاهش تورم» این رکورد موفقیت را تضعیف می‌کند. آن لایحه که ازطریق فرآیند آشتی حزبی تصویب شد، با وجود تخصیص صدها میلیارد دلار به صنایعی ازجمله وسایل نقلیه برقی و انرژی‌های تجدیدپذیر که به‌شدت در برابر حملات سایبری آسیب‌پذیر هستند، حتی یک بار در ۳۰۰ صفحه به امنیت سایبری اشاره نکرد.

این را با لایحه سرمایه‌گذاری در زیرساخت و مشاغل مقایسه کنید. در آن لایحه سرمایه‌گذاری‌های خاصی در امنیت سایبری ازجمله یک برنامه کمک مالی ۱ میلیارد دلاری برای رسیدگی به خطرات امنیت سایبری که دولت‌های ایالتی و محلی با آن مواجه هستند، انجام می‌دهد. برای بخش انرژی، دو برنامه کمک هزینه ۲۵۰ میلیون دلاری ویژه امنیت سایبری وجود دارد. یک برنامه از خدمات شهری و روستایی برای رسیدگی به مسائل شناخته‌شده امنیت سایبری و برنامه دیگر از توسعه فناوری‌های امنیت سایبری در بخش انرژی حمایت می‌کند.

قانون کاهش تورم بدون نقص نبوده و فرصت‌هایی را برای تأمین مالی بهبود امنیت سایبری در بخش‌های آب، بخش‌های حمل‌ونقل (مانند خط لوله، حمل‌ونقل دریایی، و هوانوردی) و بخش‌های مراقبت‌های بهداشتی و سلامت عمومی از دست می‌دهد. درحالی‌که قانون سرمایه‌گذاری زیرساخت و مشاغل، امنیت سایبری را به سرمایه‌گذاری‌های زیرساختی حیاتی گره می‌زند.

عنوان	Partisan Bills Hurt Cybersecurity
نویسنده	RADM (Ret) Mark Montgomery, Annie Fixler
مرکز مطالعاتی	FDD
تاریخ انتشار	December 19, 2022

پایان

زاویه

نگاهی نو،
به حکمرانی فضای مجازی

نشانی: تهران، ضلع غربی میدان فلسطین، خیابان آیت‌الله طالقانی، پلاک ۳۹۷
تلفن: ۸۶۰۵۴۲۹۱-۰۲۱
وبسایت: www.zaviehmag.ir
شبکه‌های اجتماعی: @zaviehmag

Designed by Hossein Razaqnejad | ho3inr@gmail.com