



دوره اول
شماره ۷

رصدنامه حکمرانی سایبری

مروری بر اندیشه‌های شاخص جهان | دی ۱۴۰۱



دوره ۱، شماره ۷، دی ۱۴۰۱

رصدنامه حکمرانی سایبری

مروری بر اندیشه‌های شاخص جهان



امیرعباس رکنی
امین زاده حسین

تهیه و تنظیم
ناظر علمی



تهران، ضلع غربی میدان فلسطین،
خیابان آیت الله طالقانی، پلاک ۳۹۷
۰۲۱-۸۶۰۵۴۲۹۱
www.sccm.ir

نشانی

تلفن
وبسایت



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



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



مقدمه



اندیشکده‌های شاخص جهان به جهت تعیین الگو و ارائه خط‌مشی در حوزه حکمرانی فضای مجازی به تصمیم‌سازان، اطلاع از جزئیات تحولات جاری حکمرانی فضای مجازی، پالایش و بومی‌سازی محتوای اندیشکده‌های جهان متناظر با نیازهای داخل کشور و...، نهادهای علمی و راهبردی حائز اهمیت و برجسته‌ای به شمار می‌روند. بر همین مبنا، لزوم توجه به محتوای تولیدی از سوی این مراکز مطالعاتی، امری ضروری است.

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 از جمله 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:

اهم اندیشکده‌های غیرآمریکایی

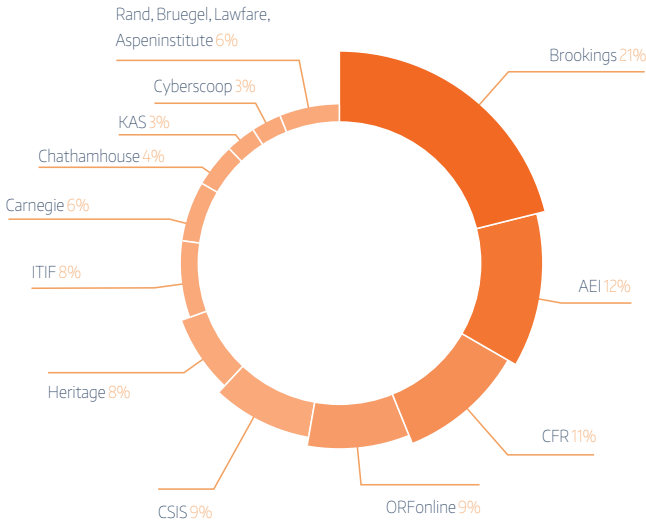
- چتم‌هاوس
- بروگل
- موسسه امور بین‌الملل و اروپا
- بنیاد فناوری اطلاعات و نوآوری
- مرکز مطالعات سیاست‌اروپا

اهم اندیشکده‌های آمریکایی

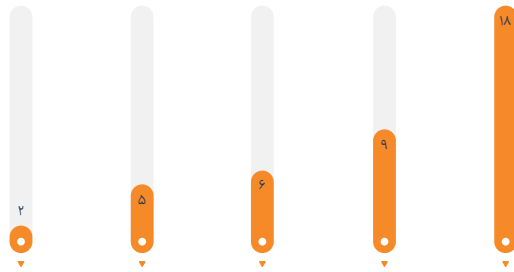
- امریکن اینترپرایز
- بروکینگز
- هریتیج
- شورای آتلانتیک
- پلفر
- ژند
- کارنگی
- پیو
- ویلسون
- شورای روابط خارجی
- موسسه اقتصاد بین‌الملل پیترسون
- موسسه هادسون
- مرکز مطالعات استراتژیک و بین‌المللی

در این شماره از رصد؛ که در بازه یک‌ماهه دی‌ماه نگارش شده است، ۶۳ عنوان استخراج شد که شامل گزارش، یادداشت، پروژه‌های تحقیقاتی و... می‌شود.

باتوجه به نمودار بالا، بروکینگز «Brookings» با ۲۱ درصد بیشترین محتوای تولیدی مرتبط با فضای مجازی را به خود اختصاص داد و بعد از آن امریکن اینترپرایز «AEI» با ۱۲ درصد، شورای روابط خارجی «CFR» با ۱۱ درصد، بنیاد آیزنبر «ORFonline» و مرکز مطالعات استراتژیک و بین‌المللی «CSIS» هرکدام با ۹ درصد، هریتیج «Heritage» و بنیاد نوآوری و فناوری اطلاعات «ITIF» هرکدام با ۸ درصد، کارنگی «Carnegie» با ۶ درصد، چتم‌هاوس «Chathamhouse» با ۴ درصد، بنیاد کنراد آدناور «KAS» و سایبراسکوپ «Cyberscoop» هرکدام با ۳ درصد و سایر اندیشکده‌ها، مشترکاً در تولید ۶ درصد از محتوا، سهیم بوده‌اند.



مطالب مستخرج، طبق یک طبقه‌بندی موضوعی که از پیش تعیین شده بود؛ در دسته‌های هوش مصنوعی، جنگ اطلاعاتی و امنیت سایبری، قانون‌گذاری و تنظیم‌گری، نیمه‌هایها و حکمرانی سایبری تقسیم شدند که فراوانی مطالب هر دسته موضوعی، به شرح ذیل است:



بیست و چهار عنوان انتخابی از اندیشکده‌های شاخص جهان در دی‌ماه، دربرگیرنده بیش از ۱۳۳ هزار کلمه محتوا می‌باشد که توسط ۱۰۵ 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 ۲۴ عنوان برگزیده از ۶۳ گزارش استخراج‌شده پرداخته شده است.



گزارش‌های برگزیده



هوش مصنوعی

چالش هوش مصنوعی مولد و خلاقیت انسانی

در این مقاله، نویسندگان توضیح می‌دهند که چگونه توسعه فناوری دیجیتال منجر به ایجاد اشکال جدیدی از هنر، مانند خلاقیت مشتق جمعی (ADC) شده است که شامل ترکیب آثار موجود برای خلق چیزی جدید است. مدت‌ها تصور بر این بود که خلاقیت، تفکر مستقل و هنر وجه متمایز بین انسان و فناوری است و فناوری، حتی در بهترین شرایط، صرفاً یک ابزار خواهد بود. آدا لاولیس^۱ یکی از نظریه‌پردازان در این باره می‌گوید: «اگر رایانه‌ها فقط می‌توانند کاری را انجام دهند که برای آن برنامه‌ریزی شده‌اند، پس نمی‌توان رفتار آن‌ها را خلاقانه نامید». او تأکید می‌کند که یادگیری مستقل یکی از ویژگی‌های اساسی خلاقیت است که فناوری هرگز نمی‌تواند واجد این ویژگی شود.

اخیراً ظهور هوش مصنوعی مولد^۲ تحقیقات لاولیس را به چالش می‌کشد. هوش مصنوعی مولد یک سیستم هوش مصنوعی است که بر روی محتوای منبع‌باز و مجموعه داده‌های تاریخی برای تولید خروجی‌های خلاقانه جدید و منحصربه‌فرد آموزش دیده است. طیف وسیعی از ابزارهای تجاری هوش مصنوعی مولد که در سال گذشته تولید شده‌اند، باهدف خودکارسازی و خودآموزی مجموعه‌ای از وظایف که از لحاظ تاریخی با ظرفیت انسانی مرتبط بوده‌اند، طراحی شده‌اند.

الگوریتم gen-AI با استفاده از سبک‌های هنرمندان، یک اثر کاملاً جدید تولید می‌کند. این اتفاق اغلب بدون رضایت هنرمندان اصلی و عدم پرداخت هزینه به هنرمندان انجام می‌شود. در نتیجه، هنرمندان و دیگر متخصصان خلاق تصور می‌کنند که gen-AI یک تهدید وجودی نه تنها برای شغل آن‌ها بلکه برای یک مهارت «انسانی» یعنی خلاقیت است.

نویسنده استدلال می‌کند که ADC سؤالات مهمی را در مورد حق چاپ و مالکیت و همچنین ماهیت خود خلاقیت مطرح می‌کند. این مقاله به بررسی پیامدهای قانونی و اخلاقی ADC، از جمله مسائل مربوط به حقوق مالکیت معنوی و پتانسیل بهره‌برداری از آثار هنرمندان می‌پردازد. نویسندگان پیشنهاد می‌کنند که برای پذیرش کامل پتانسیل ADC به‌عنوان شکل جدیدی از بیان خلاق، ممکن است رویکردی ظریف‌تر به حق چاپ لازم باشد. نویسندگان همچنین مفاهیم فلسفی ADC را بررسی کرده و این سؤال را مطرح می‌کنند که آیا خلق چیزی جدید از طریق ترکیب آثار موجود واقعاً می‌تواند اصیل یا خلاقانه در نظر گرفته شود؟

۱. Aggregative, derivative, creative (ADC)

۲. Ada Lovelace

۳. gen-AI



Aggregative, derivative, creative: Generative AI and human creativity
Shimona Mohan, Varya Srivastava
ORFonline
January 6, 2023

عنوان
نویسنده
مرکز مطالعاتی
تاریخ انتشار



آینده اخلاق در هوش مصنوعی

این مقاله در خصوص اهمیت توسعه و استقرار مسئولانه فناوری هوش مصنوعی (AI) و اینکه چگونه تأمین مالی آن می‌تواند در دستیابی به این هدف نقش داشته باشد، بحث می‌کند. نویسنده استدلال می‌کند که هوش مصنوعی قابل توضیح (XAI) می‌تواند به شفاف‌تر و پاسخگوتر شدن هوش مصنوعی کمک کند؛ امری که برای اطمینان از استفاده اخلاقی از این فناوری ضروری است. پیشرفت سریع هوش مصنوعی و یادگیری ماشین در بخش‌های مختلف منجر به جایگزینی تدریجی الگوریتم‌های داده («data algorithms») به جای تصمیم‌گیری انسانی شده است. در سال گذشته ۴۲ درصد از شرکت‌ها در سراسر جهان، کاوش خود را پیرامون پذیرش هوش مصنوعی گزارش کرده‌اند. این امر نشان‌دهنده‌ی آن است که الگوریتم‌ها بیش از هر زمان دیگری بر زندگی روزمره ما کنترل دارند.

پردازش خودکار به معنای تصمیم‌گیری سریع‌تر و کارآمدتر است که می‌تواند میزان دقت نتایج را افزایش داده و درعین حال هزینه‌ها را کاهش دهد؛ اما این مزایا با نگرانی‌های جدی در مورد سوگیری‌ها و آسیب‌های مصرف‌کننده همراه است. داده‌های ناقص، داده‌های غیر نماینده از جامعه یا دارای سوگیری‌های تاریخی منعکس شده در آن، منجر به الگوریتمی می‌شود که الگوهای غیرواقعی را بازتولید می‌کند. آزمایشی توسط «AlgorithmWatch» نشان داد که گوگل تصویر دامسج در دست یک سپاه‌پوست را به‌عنوان یک تفنگ برچسب‌گذاری کرد درحالی‌که تصویر دامسج در دست سفیدپوست را یک دستگاه الکترونیکی برچسب‌گذاری کرده است. از آنجایی‌که افراد سپاه‌پوست را بیشتر در صحنه‌های خشونت‌آمیز به تصویر می‌کشند، استنباط انجام‌شده توسط رایانه این بود که پوست تیره را با خشونت مرتبط کند. هنگامی که فناوری‌ها برای اهدافی مانند ابزارهای تشخیص سلاح در فضاهای عمومی به کار می‌روند سبب ایجاد چنین خطاهایی در دنیای واقعی می‌شوند.

یکی از مستقیم‌ترین راه‌ها برای جلوگیری از آسیب‌های مصرف‌کننده و تسهیل اصول فوق‌الذکر، ایجاد مسئولیت‌پذیری در سامانه‌ها از طریق رویکردهای توضیح‌پذیری از طریق طراحی در هوش مصنوعی است. توضیح‌پذیری به توانایی ارائه دلایل



روشن، قابل درک و قابل توجیه برای تصمیمات یا اقدامات یک الگوریتم اشاره دارد. این شامل عملکرد سیستم (منطق پشت عملیات کلی الگوریتم) و تصمیمات خاص (منطق تصمیمات خاص) است که به سازندگان، کاربران و تنظیم‌گران اجازه می‌دهد تا تعیین کنند که آیا تصمیمات گرفته‌شده در این الگوریتم منصفانه هستند یا خیر. اگرچه توضیح‌پذیری در بطن هوش مصنوعی اخلاقی قرار دارد اما استانداردی بسیار دشوار است، زیرا نیازمند بهره‌مندی از چندین رشته و تخصص مختلف است و همچنین هزینه‌های پنهانی را به همراه دارد. نگرانی اصلی در این باب، جلوگیری از عملکرد مطلوب با اجرای توضیح‌پذیری است.

این مقاله مزایای بالقوه XAI مانند بهبود اعتماد به سامانه‌های هوش مصنوعی، امکان تصمیم‌گیری بهتر و کاهش خطر عواقب ناخواسته را پررنگ می‌کند. نویسندگان خاطرنشان می‌کنند که تأمین مالی می‌تواند ابزاری برای ترویج توسعه و پذیرش XAI باشد، زیرا سرمایه‌گذاران می‌توانند پروژه‌های XAI را اولویت‌بندی کرده و شرکت‌ها را تشویق کنند تا از اصول XAI پیروی کنند. با این حال، نویسندگان اذعان می‌کنند که تأمین مالی XAI راه‌حل نهایی نیست و چالش‌هایی وجود دارد که باید به آن‌ها رسیدگی کرد؛ مانند اطمینان از اینکه از XAI برای تداوم تعصبات و نابرابری‌های موجود استفاده نمی‌شود. نویسندگان به همین منظور خواستار همکاری میان ذی‌نفعان، از جمله دولت‌ها، شرکت‌ها، سرمایه‌گذاران و جامعه مدنی هستند تا از توسعه و استقرار XAI به شیوه‌ای اخلاقی و مسئولانه اطمینان حاصل شود.



Building an ethical AI Future through XAI financing

Amoha Basrur, Sahil Deo

ORFonline

December 29, 2022

عنوان

نویسنده

مرکز مطالعاتی

تاریخ انتشار



جنگ اطلاعاتی و
امنیت سایبری

امنیت و جنگ اطلاعاتی روسیه

بنیاد صلح بین‌المللی کارنگی، در مقاله اخیر خود نقش جنگ اطلاعاتی در تلاش‌های روسیه برای حفظ امنیت خود را تحلیل می‌کند. این مقاله استدلال می‌کند که رهبران روسیه جنگ اطلاعاتی را ابزاری ضروری برای محافظت از قدرت خود و تأثیرگذاری بر سیاست جهانی می‌دانند و رویکردی پیچیده و چند وجهی برای پروپاگاندا و انتشار اطلاعات نادرست ایجاد کرده‌اند. نویسندگان این مقاله خاطرنشان می‌کنند که رویکرد روسیه نسبت به جنگ اطلاعاتی نه تنها شامل تلاش‌های تبلیغاتی آشکار است، بلکه عملیات پنهانی برای ایجاد سردرگمی و تضعیف نهادهای دموکراتیک در کشورهای هدف را نیز شامل می‌شود. آن‌ها توضیح می‌دهند که رهبران روسیه به این عملیات به‌عنوان ابزاری برای نمایش قدرت و دفاع از منافع خود در دنیایی که در آن دامنه اقدام و عمل نیروی نظامی سنتی به‌شدت محدود است، نگاه می‌کنند.

به‌طورکلی، این مقاله ماهیت در حال تحول نبرد در قرن بیست و یکم و اهمیت فزاینده جنگ اطلاعاتی در سیاست جهانی را روشن می‌کند. درحالی‌که روسیه به توسعه توانایی‌های خود در این زمینه ادامه می‌دهد، سیاست‌گذاران در ایالات متحده و سایر کشورها باید هوشیار بوده و برای تقویت نهادهای دموکراتیک و دفاع در برابر مداخلات عوامل خارجی در امور داخلی خود تلاش کنند. دموکراسی‌ها با درک اهمیت جنگ اطلاعاتی و توسعه راهبردهای مؤثر برای مقابله با آن، می‌توانند پایداری و ثبات خود را در مواجهه با این محیط جهانی شدیداً پیچیده و چالش‌برانگیز تضمین کنند.

”



No Water's Edge: Russia's Information War and Regime Security
Gavin Wilde, Justin Sherman
Carnegie
January 4, 2023

عنوان
نویسنده
مرکز مطالعاتی
تاریخ انتشار

تمرکز بر جنگ اطلاعاتی

گاوین وایلد^۱ تحلیلگر سایبر اسکوپ، در مقاله اخیر خود توضیح می‌دهد که بر اساس آمار و گزارش‌های موجود، روسیه در فیس‌بوک مشغول یک جنگ اطلاعاتی تمام‌عیار علیه غرب است. او برای اثبات ادعای خود به بررسی کمپین‌های اطلاعات نادرست مورد حمایت روسیه در رسانه‌های اجتماعی می‌پردازد. وایلد به بررسی گزارش اخیر Graphik، یک شرکت تجزیه و تحلیل رسانه‌های اجتماعی استناد می‌کند که شواهدی از رفتار نامعتبر هماهنگ شده^۲ (CIB) در فیس‌بوک از سوی عوامل وابسته به دولت روسیه را پیدا کرده است. بر اساس این گزارش، کمپین CIB از شبکه‌ای از حساب‌ها و صفحات جعلی برای تقویت روایت‌های طرفداران روسیه و حمله به مخالفان کرملین استفاده کرده است. وایلد خاطرنشان می‌کند که این تازه‌ترین نمونه از تلاش‌های روسیه برای استفاده از رسانه‌های اجتماعی به منظور تأثیرگذاری بر افکار عمومی و تضعیف نهادهای دموکراتیک، چه در داخل و چه در خارج از کشور خود است.

او چالش‌های پیش روی پلتفرم‌های رسانه‌های اجتماعی در شناسایی و حذف کمپین‌های اطلاعات نادرست، به ویژه آن‌هایی که به خوبی هماهنگ و پیچیده هستند را نیز، مورد بحث قرار می‌دهد. او خاطرنشان می‌کند در حالی که فیس‌بوک و سایر پلتفرم‌ها گام‌هایی برای بهبود قابلیت‌های تشخیص خود برداشته‌اند، مقیاس و پیچیدگی مشکل همچنان یک چالش مهم است.

به طور کلی، گزارش گاوین وایلد تهدید مداوم ناشی از کمپین‌های اطلاعات نادرست مورد حمایت روسیه و نیاز به هوشیاری سیاست‌گذاران و شرکت‌های رسانه‌های اجتماعی را برجسته می‌کند. در پایان او استدلال می‌کند که با توسعه استراتژی‌های مؤثر برای شناسایی و مقابله با این کمپین‌ها، می‌توان به حفظ یکپارچگی نهادهای دموکراتیک و ترویج گفت‌وگو عمومی آگاهانه‌تر و فعال‌تر کمک کرد.



1. Gavin Wilde
2. Coordinated inauthentic behavior (CIB)

It's time to focus on information warfare's hard questions

Gavin Wilde

cyberscoop

January 3, 2023

عنوان
نویسنده
مرکز مطالعاتی
تاریخ انتشار



نقش دیپ فیک در جنگ‌های بین‌المللی

فریبکاری و دست‌کاری رسانه‌ای همیشه بخشی از ارتباطات دوران جنگ بوده اما پیش‌ازاین هرگز برای هیچ دولتی در یک درگیری و جنگ امکان تولید صوت، ویدیو و متن واقعی از مقامات سیاسی و رهبران نظامی مخالف خود وجود نداشته است. همان‌طور که هوش مصنوعی پیچیده‌تر شده و هزینه محاسبات را کاهش می‌دهد، چالش‌های دیپ فیک برای محیط‌های اطلاعاتی آنلاین در طول درگیری‌های مسلحانه افزایش می‌یابد. با توجه به آثار و پیامدهای مخرب و جبران‌ناپذیری که فناوری دیپ فیک می‌تواند برای امنیت جهانی داشته باشد، جمعی از پژوهشگران مؤسسه بروکینگز جدیدترین مطالعه خود را به دیپ فیک اختصاص داده‌اند. در این مقاله، نویسندگان تأثیر بالقوه دیپ فیک بر مناقشات بین‌المللی را بررسی می‌کنند. دیپ فیک‌ها تصاویر و ویدیوهای رایانه‌ای هستند که معتبر به نظر می‌رسند و پتانسیل استفاده برای اهداف مخرب مانند انتشار اطلاعات نادرست یا دست‌کاری افکار عمومی را دارند. نویسندگان استدلال می‌کنند که توسعه فناوری دیپ فیک چالش‌های جدیدی برای امنیت و ثبات بین‌المللی ایجاد کرده و در این مقاله نویسندگان راه‌های مختلفی را بیان می‌کنند که در آن‌ها می‌توان از دیپ فیک برای تحریک یا تشدید درگیری استفاده کرد.

یکی از کاربردهای بالقوه دیپ فیک در زمینه مناقشات بین‌المللی، ایجاد شواهد یا تبلیغات نادرست است که می‌تواند برای حمایت از اقدامات نظامی یا دیپلماتیک استفاده شود. برای مثال، یک ویدیوی دیپ فیک می‌تواند کشوری را در حال انجام یک اقدام تحریک‌آمیز نشان دهد، یا به نظر برسد که یک فرمانده نظامی حرفی توهین‌آمیز و جنجالی علیه دشمن خود زده است. نگرانی دیگر این است که می‌توان از دیپ فیک‌ها برای ایجاد سردرگمی یا بی‌اعتمادی میان مردم استفاده کرد و این امر رسیدن به اجماع در مورد موضوعات مهم برای کشورها را دشوارتر می‌کند. نویسندگان استدلال می‌کنند که متداول شدن دیپ فیک‌ها می‌تواند تنش‌های موجود را تشدید و تنش‌های جدیدی ایجاد کند و از این رو خواستار توجه بیشتر به این موضوع از سوی سیاست‌گذاران و کارشناسان امنیتی هستند.

برای مقابله با تهدید ناشی از دیپ فیک، نویسندگان چندین توصیه سیاستی پیشنهاد می‌کنند که به شرح ذیل است:

نخست، آن‌ها خواستار افزایش سرمایه‌گذاری در تحقیق و توسعه فناوری‌ها برای شناسایی و مبارزه با دیپ فیک هستند. دوم، آن‌ها استدلال می‌کنند که هنجارها و استانداردهای بین‌المللی باید برای تعیین اینکه چه بخشی از فناوری دیپ فیک قابل قبول است و چه بخشی قابل قبول نیست، ایجاد شود. در نهایت، نویسندگان بر اهمیت همکاری بین کشورها برای پرداختن به این موضوع، از جمله از طریق به اشتراک‌گذاری اطلاعات و بهترین شیوه‌ها تأکید می‌کنند. به‌طور کلی، مقاله خطرات و چالش‌های بالقوه ناشی از دیپ فیک‌ها را در زمینه مناقشات بین‌المللی برجسته کرده و خواستار اقدامات پیشگیرانه برای مقابله با این تهدید رو به افزایش است.



عنوان

Daniel L. Byman, Chongyang Gao, Chris Meserole, V.S. Subrahmanian

Brookings

January 10, 2023

عنوان

نویسنده

مرکز مطالعاتی

تاریخ انتشار



مداخلات اشخاص ثالث برای کاهش اطلاعات نادرست

کاربران رسانه‌های اجتماعی با وجود پیشرفت‌هایی که شرکت‌های بزرگ رسانه‌های اجتماعی در رویکردهای اجرایی و اولویت‌بندی برای رسیدگی به آسیب‌های ناشی از اطلاعات گمراه‌کننده یا نادرست آنلاین انجام داده‌اند، همچنان با اطلاعات نادرست مواجه هستند. تحقیقات نشان می‌دهد که کاربران آگاه می‌توانند سرعت انتشار اطلاعات نادرست را کاهش دهند. نتایج تحقیقات بیان می‌کند کاربران ابزارهایی را برای قضاوت اطلاعات درست از نادرست نیاز دارند، اما هنوز فاقد یک درک بنیادی از چگونگی دستیابی به این ابزار هستند. در پاسخ به این چالش‌ها، جمعی از پژوهشگران بنیاد کارنگی در جدیدترین مقاله خود، اقدام به بررسی تأثیر مداخله اشخاص ثالث در فرایند مبارزه با اخبار جعلی نمودند.

مقاله با تشریح اشکال مختلف اطلاعات نادرست، مانند اطلاعات غلط، محتوای گمراه‌کننده و رسانه‌های دستکاری‌شده آغاز می‌شود. سپس تأثیر اطلاعات نادرست، از جمله از بین بردن اعتماد به مؤسسات و آسیب رساندن به سلامت عمومی را مورد بحث قرار می‌دهد. نویسندگان خاطرنشان می‌کنند که علی‌رغم اثرات منفی آشکار اطلاعات نادرست، مداخلات برای مبارزه با آن تأثیر محدودی داشته است. یکی از چالش‌ها در اجرای مداخلات مبتنی بر شواهد، فقدان اجماع در مورد چگونگی اندازه‌گیری اثربخشی آن‌ها است. نویسندگان توضیح می‌دهند که برای ارزیابی تأثیر مداخلات، نیاز به معیارهای بهتری داریم، مانند نظرسنجی‌ها و آزمایش‌هایی که می‌توانند تغییرات در رفتار و نگرش‌ها را اندازه‌گیری کنند. این مقاله ابتکاراتی که به دنبال توسعه چنین معیارهایی بوده‌اند، مانند پروژه اعتماد و ابتکار یکپارچگی اخبار را برجسته می‌کند.

چالش دیگر نیاز به همکاری در بخش‌های مختلف از جمله دولت، جامعه مدنی و بخش خصوصی است. نویسندگان تأکید می‌کنند که مداخلات مؤثر نیاز به تلاش هماهنگ در این بخش‌ها و همچنین مشارکت مردم دارد. در این مقاله چندین مورد

از ابتکاراتی که به دنبال ارتقاء چنین همکاری‌هایی هستند، مانند شاخص جهانی اطلاعات و کارگروه عالی تعدیل محتوای آنلاین ترانس آتلانتیک^۲ مورد بحث قرار گرفته است.

در این مقاله نیاز به شفافیت بیشتر در مداخلات جهت مبارزه با اطلاعات نادرست، ضروری تلقی شده است. نویسندگان خاطرنشان می‌کنند که بسیاری از ابتکارات به دلیل عدم شفافیت و پاسخگویی با انتقاد روبرو شده‌اند، که این مسئله می‌تواند اعتماد عمومی را تضعیف کند. در این مقاله چندین ابتکار عمل که به دنبال رسیدگی به این موضوع بوده‌اند، مانند ابتکار اعتماد روزنامه‌نگاری و پروژه بهبود رسانه‌ها^۳، برجسته شده است.

۲. Global Disinformation Index and the Transatlantic High Level Working Group on Content Moderation Online.

۳. Journalism Trust Initiative and the Media Well-being Project.



Evidence-Based Misinformation Interventions: Challenges and Opportunities for Measurement and

عنوان

Collaboration

Yasmin Green, Andrew Gully, Yoel Roth, Abhishek Roy, Joshua A. Tucker, Alicia Wanless

نویسنده

Carnegie

مرکز مطالعاتی

January 9, 2023

تاریخ انتشار

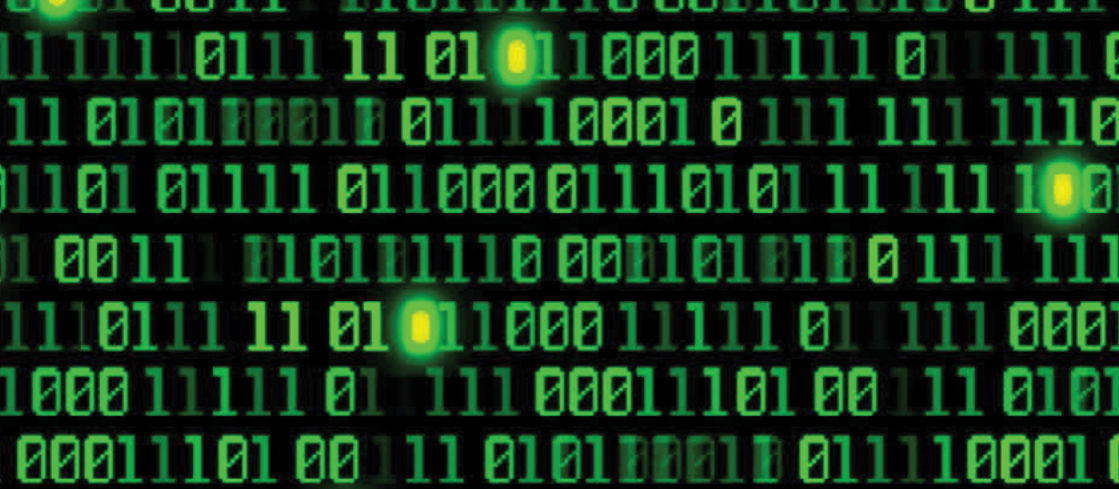


بزرگ‌ترین کنفرانس هک در روسیه

در ماه می سال گذشته حدود ۸۷۰۰ هکر، توسعه‌دهنده و شرکت امنیت سایبری در روسیه برای شرکت در یکی از بزرگ‌ترین کنفرانس‌های هکری این کشور به نام «Positive Hack Days» در مسکو گرد هم آمدند. «Positive Hack Days» که از سال ۲۰۱۱ هر ساله برگزار می‌شود از بسیاری جهات یادآور رویدادهای امنیت سایبری آمریکا مانند «Defcon» یا «Blackhat» است. کنفرانس «Positive Hack Days» توسط شرکت امنیت سایبری روسی به نام «Positive Technologies» که دولت ایالات متحده آن را در آوریل ۲۰۲۱ به دلیل حمایت از عملیات سایبری دولت روسیه تحریم کرد، سازمان‌دهی شده است. بر اساس گزارش‌ها، این شرکت ضمن کشف آسیب‌پذیری‌ها در محصولات فناوری، برای آن آسیب‌پذیری‌ها راه‌حل می‌یابد و آن‌ها را در اختیار سرویس امنیت فدرال روسیه (FSB) قرار می‌دهد.

اگرچه برنامه‌ها و بحث‌های آخرین دوره از کنفرانس Positive Hack Days بر ملی‌گرایی و اهمیت بخش فناوری داخلی روسیه متمرکز بود، برخی از شرکت‌کنندگان نگرانی‌های مرتبط با انزوای فناوری روسیه را بیان کردند. با این حال بسیاری دیگر (به‌ویژه کسانی که از تحریم‌ها و انزوای فناوری به‌عنوان فرصتی برای گسترش محصولات و خدمات امنیت سایبری خود استفاده کرده‌اند)، از دولت پوتین حمایت کردند.

جاستین شرمین، در مقاله‌ای که در بروکینگز به همین مناسبت نوشته، این رویداد را دلیلی بر انزوای فناوری روسیه و چگونگی دست‌وپنجه نرم کردن جامعه امنیت سایبری روسیه با انزوای فزاینده، تحریم‌های غرب و مشکلات اقتصادی ناشی از عدم فروش محصولات نرم‌افزاری و سخت‌افزاری روسی در بازار جهانی کنونی می‌داند. او تأکید می‌کند که سیاست‌گذاران غربی باید بدانند که متخصصان سایبری روسیه به‌وضوح اثرات تحریم‌های جدید را احساس می‌کنند، چراکه کارشناسان فناوری در روسیه به‌وضوح در این کنفرانس درباره پیامدها و راه‌حل‌های جایگزین صحبت کردند.



این مقاله نشان می‌دهد که چگونه اکوسیستم سایبری روسیه با اعمال کنترل بیشتر بر فعالیت‌های آنلاین و محدود کردن دسترسی به فناوری‌های خارجی، شدیداً منزوی شده و این امر منجر به شکاف دیجیتالی فزاینده بین روسیه و غرب شده است، به طوری که هکرهای روسی و کارشناسان امنیت سایبری به آخرین فناوری‌ها و دانش مشترک در رویدادهای مشابه در ایالات متحده و اروپا دسترسی ندارند. این مقاله نشان می‌دهد که این انزوا نظارت و کنترل فعالیت‌های آنلاین را برای سرویس‌های امنیتی روسیه آسان‌تر کرده و به طور بالقوه منجر به استبداد و سانسور بیشتر می‌شود.

نویسنده خاطرنشان می‌کند در حالی که جامعه هکرهای این کشور نیرویی ماهر و مبتکر است، کار آن‌ها اغلب توسط دولت و برای نیل به اهداف سیاسی انتخاب می‌شود. شرم‌نقش گروه‌های هکری تحت حمایت دولت در حملات سایبری اخیر را نیز برجسته می‌کند. این مقاله با اشاره به چالش‌های ناشی از اکوسیستم سایبری منزوی روسیه، از جمله پتانسیل افزایش تنش‌های ژئوپلیتیکی و محدودیت همکاری بین‌المللی در خصوص مسائل امنیت سایبری، به پایان می‌رسد. شرم‌نقش پیشنهاد می‌کند که جامعه بین‌المللی برای ترویج شفافیت و همکاری بیشتر، نیاز دارد بیشتر با جامعه هکر روسیه تعامل کند و در عین حال دولت روسیه را در قبال فعالیت‌های سایبری خود مسئول بداند.



Russia's largest hacking conference reflects isolated cyber ecosystem
Justin Sherman
Brookings
January 12, 2023

عنوان
نویسنده
مرکز مطالعاتی
تاریخ انتشار



آینده جنگ سایبری در اقیانوس هند و آرام

در اجلاس ژوئن ۲۰۲۲ ناتو با حضور استرالیا، نیوزیلند، ژاپن و کره جنوبی تهدیدهای سایبری و استفاده مخرب چین از این ظرفیت مورد توجه قرار گرفت. در این اجلاس، همچنین نگرانی‌هایی مبتنی بر الگوبرداری چین از مبارزات دیجیتال ارتش روسیه ابراز شد؛ در نتیجه شورای مشارکت یورو آتلانتیک (Euro-Atlantic) به منظور سرمایه‌گذاری مجدد همبستگی سیاسی برای دفاع سایبری تصمیماتی را اتخاذ و به نقش جنگ سایبری و استفاده از ابزارهای ICT در منطقه هند و اقیانوس آرام تأکید کرده است.

در همین خصوص، بارت هوگین در جدیدترین مقاله خود با عنوان «آینده جنگ سایبری در هند و اقیانوس آرام» که توسط بنیاد تحقیقاتی آبرور منتشر شده است، تحلیلی عمیق از وضعیت کنونی جنگ سایبری در منطقه هند و اقیانوس آرام و سناریوهای بالقوه‌ای که ممکن است در سال‌های آینده در این منطقه رخ دهد، ارائه می‌کند. نویسنده استدلال می‌کند که منطقه هند و اقیانوس آرام به دلیل میزان بالای اتصال و اتکا به فناوری در برابر حملات سایبری آسیب‌پذیر است. علاوه بر این، فقدان رویکرد یکپارچه برای امنیت سایبری و وجود تنش‌های ژئوپلیتیکی و درگیری‌های تاریخی خطر جنگ سایبری را در این منطقه تشدید می‌کند. این مقاله چندین عامل کلیدی مؤثر در جنگ سایبری در اقیانوس هند و اقیانوس آرام را شناسایی کرده است. این موارد شامل عدم تقارن قدرت بین بازیگران اصلی، عدم شفافیت و پاسخگویی در فضای سایبری و استفاده از عوامل غیردولتی و نیابتی برای انجام حملات سایبری است.

نویسنده همچنین اشکال مختلف جنگ سایبری که در حال حاضر در منطقه وجود دارد، مانند جاسوسی، خرابکاری و تبلیغات را بررسی می‌کند. او خاطرنشان می‌کند که این تاکتیک‌ها اغلب برای هدف قرار دادن زیرساخت‌های حیاتی و دارایی‌های استراتژیک مانند پایگاه‌های نظامی، مؤسسات مالی و شبکه‌های انرژی استفاده می‌شود. یکی از استدلال‌های اصلی مقاله این است که جنگ سایبری احتمالاً در سال‌های آینده شدیداً در منطقه هند و اقیانوس آرام رایج و پیچیده خواهد شد. نویسنده از سرعت سریع پیشرفت فناوری، تعداد زیاد بازیگران سایبری و ظهور اشکال جدیدی از تهدیدات سایبری به عنوان محرک‌های اصلی این روند یاد



می‌کند. برای پرداختن به این چالش، مقاله تعدادی توصیه سیاستی را پیشنهاد می‌کند. توسعه مجموعه‌ای از هنجارها و قوانین رفتاری مشترک در فضای سایبری، ایجاد چارچوب امنیت سایبری منطقه‌ای و ایجاد یک فرماندهی سایبری اختصاصی برای منطقه از جمله این موارد است.

این مقاله همچنین نیاز به مساعدت و همکاری بین‌المللی برای مقابله با تهدیدات رو به تغییر در حوزه سایبری را مورد بحث قرار می‌دهد. نویسنده استدلال می‌کند که با توجه به ماهیت فراملی تهدیدات سایبری، تلاش هماهنگ دولت‌ها، نهادهای بخش خصوصی و سایر ذی‌نفعان برای توسعه سیاست‌ها و استراتژی‌های مؤثر در کاهش خطرات ناشی از عملیات سایبری ضروری است. علاوه بر این، این مقاله پیشنهاد می‌کند که کشورهای منطقه باید برای توسعه قابلیت‌های سایبری خود، اعم از تدافعی و تهاجمی، سرمایه‌گذاری کنند تا از خود در برابر دشمنان احتمالی و از منافع خود در فضای سایبری دفاع کنند. به‌طور کلی، این مقاله مروری جامع از وضعیت کنونی جنگ سایبری در منطقه هند و اقیانوس آرام ارائه می‌کند و نیاز به یک رویکرد هماهنگ و فعالانه برای امنیت سایبری را برجسته می‌کند. تحلیل نویسنده به خوبی با شواهد موجود پشتیبانی می‌شود و بینش ارزشمندی در مورد پویایی پیچیده فضای مجازی در این منطقه مهم را ارائه می‌دهد.



The Future of Cyber Warfare in the Indo-Pacific
Bart Hogeveen
ORFonline
January 13, 2023

عنوان
نویسنده
مرکز مطالعاتی
تاریخ انتشار



قانون گذاری و
تنظیم گری

حذف مفاد «قانونی اما مضر» از لایحه اصلاح شده ایمنی آنلاین بریتانیا

مارک مکاری پژوهشگر مؤسسه بروکینگز، در مقاله «دولت بریتانیا مفاد قانونی اما مضر را از لایحه اصلاح شده ایمنی آنلاین خود حذف می‌کند»، تغییرات اخیر در تلاش‌های بریتانیا برای تنظیم محتوای آنلاین را بررسی می‌کند. او به‌طور خاص درباره حذف چندین ماده بحث برانگیز از لایحه ایمنی آنلاین پیشنهادی بریتانیا که به دلیل نقض بالقوه آزادی بیان و محدود کردن بیان آنلاین مورد انتقاد قرار گرفته بود، صحبت می‌کند.

مکاری خاطر نشان می‌کند با وجود اینکه لایحه اصلاح شده همچنان شامل اقداماتی برای رسیدگی به محتوای مضر و بهبود ایمنی آنلاین است، حذف این مقررات گامی مثبت در جهت اطمینان از ایجاد تعادل بین مقررات و آزادی بیان است. این تحلیل‌گر اذعان می‌کند که تمایل دولت بریتانیا برای بازنگری در این لایحه در پاسخ به نگرانی‌های عمومی، اهمیت مشارکت در گفتگوی عمومی در خصوص تنظیم محتوای آنلاین را نشان می‌دهد. اصلاحات پیشنهادی مطرح شده به شرح ذیل است:

- محتوای قانونی اما مضر برای بزرگسالان حذف شود.
- مکانیسم‌هایی برای کاربران فراهم شود تا از قرار گرفتن در معرض برخی از مصادیق ذکر شده در لایحه مانند سخنان نفرت‌انگیز یا تشویق به خودآزاری دور بمانند.
- تشویق به خودآزاری؛ هرزه‌نگاری دیپ‌فیک^۱ و عکس اندام جنسی از روی لباس و بدون رضایت^۲ جرم‌انگاری شود.
- شرکت‌های رسانه‌های اجتماعی ملزم شوند که محتوا را فقط در صورت غیرقانونی بودن یا نقض استانداردهای اعلام شده عمومی حذف کنند و نظام‌هایی برای اجرای استانداردهای اعلام شده عمومی خود داشته باشند. همچنین برای کاربرانی که محتوای آن‌ها حذف شده است، فرایند تجدیدنظر ارائه کنند.

به‌طور کلی، تحلیل مکاری بر اهمیت توجه دقیق در تنظیم محتوای آنلاین تأکید می‌کند. با وجود اینکه اقداماتی برای رسیدگی به محتوای مضر قطعاً ضروری است، سیاست‌گذاران باید از عدم نقض حق آزادی بیان افراد با انجام این اقدامات اطمینان حاصل کنند. دولت‌ها می‌توانند با آغاز یک گفتگوی عمومی و تجدیدنظر در پیشنهادها در پاسخ به نگرانی‌های عمومی، تعادل مناسبی بین مقررات و آزادی بیان ایجاد کنند و در نهایت یک محیط آنلاین بازتر و فراگیرتر را ترویج نمایند.

۱. Encouragement to self-harm
۲. Deepfake pornography
۳. Downblousing



U.K. government purges "legal but harmful" provisions from its revised Online Safety Bill
Mark MacCarthy
Brookings
December 21, 2022

عنوان
نویسنده
مرکز مطالعاتی
تاریخ انتشار



هند و تنظیم‌گری ارزهای دیجیتال

این مقاله استدلال می‌کند که مشارکت هند در نشست‌های گروه ۲۰ درباره مقررات ارزهای دیجیتال بسیار مهم است؛ زیرا این کشور سهم قابل توجهی در بازار جهانی ارزهای دیجیتال دارد. هند دومین بازار بزرگ ارزهای رمزنگاری شده در جهان است و تخمین زده می‌شود که ۱۵ میلیون سرمایه‌گذار در این کشور دارای بیش از ۶۶ میلیارد دلار دارایی دیجیتال هستند؛ بنابراین، هرگونه اقدامات نظارتی اتخاذشده توسط کشورهای گروه ۲۰ تأثیر قابل توجهی بر صنعت ارزهای دیجیتال هند خواهد داشت. گیتا گوپیناث، معاون مدیرعامل صندوق بین‌المللی پول، معتقد است که در دوران ریاست هند بر گروه ۲۰ این فرصت وجود دارد که در موضوع حیاتی تنظیم‌گری رمزارزها، شاهد پیشرفت چشم‌گیری باشیم. ارزهای دیجیتال به‌گونه‌ای طراحی شده‌اند که غیرمتمرکز باشند. با این حال، با وجود ماهیت غیرمتمرکز رمزارزها، این صنعت به‌سوی متمرکز شدن پیش رفته است. قسمت بزرگی از بازار ارزهای دیجیتال توسط صرافی‌های اصلی مانند FTX، بایننس و کوین‌بیس اداره می‌شوند. دلایل متعددی وجود دارد که چرا این حرکت به سمت ایجاد تمرکز رخ داده است؛ یک دلیل این است که به‌طور کلی اداره نهادهای متمرکز آسان‌تر است. صرافی‌های متمرکز می‌توانند طیف وسیع‌تری از ویژگی‌ها و خدمات مانند معاملات حاشیه و قراردادهای آتی را ارائه دهند و معاملات را سریع‌تر و کارآمدتر از صرافی‌های غیرمتمرکز پردازش کنند. از سوی دیگر صرافی‌های غیرمتمرکز تراکنش‌ها را آهسته‌تر، دشوارتر و با هزینه‌های بالاتر اجرا می‌کنند.

اما موضع هند در مورد ارزهای دیجیتال چیست؟ در سال ۲۰۱۳ بانک مرکزی هند بیانیه‌ای صادر کرد که در آن به کاربران، دارندگان و معامله‌گران ارزهای دیجیتال درباره خطرات احتمالی مرتبط با استفاده از آن‌ها هشدار داد. در سال ۲۰۱۷ بانک مرکزی هند بخشنامه‌ای را صادر کرد که در آن بانک‌ها و سایر نهادهای تحت نظارت، از ارائه خدمات به معامله‌گران رمزارزها منع شدند. این بخشنامه عملاً خرید یا فروش ارزهای دیجیتال را برای ساکنان هند غیرقانونی اعلام کرد.

باین‌حال در مارس ۲۰۲۰ دادگاه عالی هند ممنوعیت اعلام‌شده توسط بانک مرکزی هند در مورد ارزهای رمزنگاری‌شده را لغو نموده و اعلام کرد که این ممنوعیت نقض حقوق اساسی شهروندان است. این تصمیم عملاً استفاده از ارزهای رمزنگاری‌شده را در هند قانونی کرد و راه را برای پذیرش گسترده‌تر آن‌ها باز کرد. در سال ۲۰۲۲ وزارت دارایی هند گزارشی منتشر کرد که در آن پیشنهاد ایجاد رویه دیجیتال تحت حمایت دولت و همچنین چارچوبی برای تنظیم ارزهای دیجیتال خصوصی را ارائه کرد. این گزارش همچنین ایجاد یک مرجع تنظیم ارز دیجیتال (DCRA) را برای نظارت بر استفاده از ارزهای دیجیتال در هند توصیه می‌کند.

این مقاله پیشنهاد می‌کند که هند باید برای اتخاذ یک رویکرد متعادل در خصوص مقررات ارزهای دیجیتال که خطرات را برطرف کرده و در عین حال امکان نوآوری در این بخش را نیز فراهم می‌کند، تلاش کند. هند همچنین باید با سایر کشورهای گروه ۲ همکاری کند تا رویکردی هماهنگ برای مقررات ارزهای دیجیتال ایجاد کند که زمینه بازی برابر را برای همه شرکت‌کنندگان در بازار تضمین نماید. علاوه بر این، هند باید از تخصص خود در فناوری و نوآوری به منظور کمک به توسعه استانداردهای جهانی برای مقررات ارزهای دیجیتال استفاده کند. به طور کلی، این مقاله بر اهمیت مشارکت فعال هند در بحث‌های گروه ۲- در مورد مقررات ارزهای دیجیتال برای محافظت از منافع این کشور در این بخش شش‌گانه در حال تحول تأکید می‌کند.



The G20 and India's role in cryptocurrency regulation

Sauradeep Bag

ORFonline

January 5, 2023

عنوان

نویسنده

مرکز مطالعاتی

تاریخ انتشار

جنبه‌های رقابت و انحصار در قانون پیشنهادی داده اتحادیه اروپا

قانون پیشنهادی داده اتحادیه اروپا (Data Act) به کاربران حق دسترسی و قابلیت حمل داده‌های تولیدشده توسط آن‌ها از محصولات و دستگاه‌های دیجیتال ملموس را می‌دهد. این اقدام رقابت‌جویانه، کنترل انحصاری تولیدکنندگان محصول را بر داده‌های تولیدشده توسط محصول کاهش می‌دهد. باین حال قانون داده همچنین به تولیدکنندگان حق قانونی برای قیمت‌گذاری انحصاری انتقال داده به ارائه‌دهندگان خدمات شخص ثالث را می‌دهد و کنترل آن‌ها را بر بازارهای داده میسر می‌کند. سایر مقررات ضد رقابتی این قانون، شامل محدودیت در استفاده از داده‌ها برای مقاصد رقابتی و ممنوعیت انتقال داده‌ها به پلتفرم‌هایی می‌شود که طبق قانون بازارهای دیجیتال اتحادیه اروپا به‌عنوان دروازه‌بان، شناسایی شده‌اند. تعاریف غیرضروری مبهم از محصولات و داده‌هایی که تحت حاکمیت قانون داده‌ها قرار می‌گیرند، باعث ایجاد عدم اطمینان در اجرا و عدم انسجام با سایر مقررات داده‌های اتحادیه اروپا شده است.

برترین مارتنز، در مقاله اخیر خود در مؤسسه بروکینگز، مفاد قانون داده اتحادیه اروپا را که می‌تواند اثرات مثبت یا ضد رقابتی داشته باشد، بررسی می‌کند. او استدلال می‌کند با اینکه این قانون پتانسیل افزایش رقابت و نوآوری را دارد، در صورتی که برخی مقررات به‌طور مؤثر اجرا نشود، می‌تواند منجر به تمرکز در بازار شود. نویسنده تأکید می‌کند که یکی از اهداف کلیدی قانون داده افزایش دسترسی به داده‌ها برای مشاغل و محققان است که می‌تواند منجر به نوآوری و رقابت بیشتر شود. باین حال، خاطرنشان می‌کند که این قانون شامل مقرراتی هم می‌باشد که به‌طور بالقوه می‌تواند رقابت را محدود کند؛ مواردی چون قابلیت حمل داده. مارتنز پیشنهاد می‌کند که بررسی دقیقی نیاز است تا اطمینان حاصل شود که این مقررات ناخواسته به نفع شرکت‌های بزرگ نبوده و ورود بازیگران جدید را محدود نمی‌کند.

نویسنده استدلال می‌کند که چنین شرطی رقابت را در خدمات مبتنی بر داده افزایش می‌دهد و کاربران را از پرداخت مجدد برای داده‌های خود بازمی‌دارد. علاوه بر این، باعث بی‌انگیزگی تولیدکنندگان از سرمایه‌گذاری در محصولات و خدمات مبتنی بر داده نمی‌شود. نویسنده پیشنهاد می‌کند که گام بعدی می‌تواند ایجاد محیطی برابر بین تولیدکنندگان و کاربران در حقوق دسترسی به داده‌ها از طریق معرفی اصل استهلاک متقابل حقوق داده در محل فروش باشد. این امر همه طرفین تولیدکننده داده را در موقعیتی برای به حداکثر رساندن نوآوری و صرفه‌جویی در تجمیع داده‌ها با اثرات خارجی مبتنی بر داده قرار می‌دهد.

نویسنده در این مقاله به چند پرسش اساسی می‌پردازد. ابتدا، نویسنده بحث می‌کند که تا چه حد حق اجباری دسترسی به داده‌ها برای کاربران، کنترل انحصاری سازنده دستگاه بر داده‌های کاربر را تضعیف و رقابت در بازارهای خدمات مبتنی بر داده را باز می‌کند. این تجزیه و تحلیل بین بازارهای داده بالادستی و بازارهای خدمات داده محور پایین‌دستی، یک چشم انداز عمودی ادغام‌شده ایجاد می‌کند. این تحلیل با ارائه یک ماده موافق با رقابت در قانون داده‌ها شروع می‌شود که

به کاربران محصول یا دستگاه، حقوق دسترسی و قابلیت حمل داده‌های دستگاه را اعطا می‌کند.

نویسنده چندین مورد از مفاد ضد رقابتی را بررسی می‌کند؛ از جمله حقوق انحصاری قیمت‌گذاری داده‌های شخص ثالث برای سازندگان دستگاه و دارندگان داده و ممنوعیت استفاده از داده‌ها برای رقابت در بازارهای محصول و خدمات و انتقال داده‌ها به پلتفرم‌هایی که تحت قانون ۲۰۲۲ بازارهای دیجیتال اتحادیه اروپا^۲ به عنوان دروازه‌بان تعریف شده‌اند. نویسنده نتیجه می‌گیرد که ترکیبی از حقوق قابل حمل داده برای کاربران و حق قیمت‌گذاری داده انحصاری برای سازندگان دستگاه، تعادل در زنجیره ارزش داده‌ها را به نفع سازنده و دارنده داده به هزینه کاربران و ارائه‌دهندگان خدمات شخص ثالث تغییر می‌دهد.

علاوه بر این، نویسنده پیشنهاد می‌کند که قانون داده‌ها به اثرات شبکه مبتنی بر داده رسیدگی نمی‌کند و حقوق دسترسی به داده‌ها را، با این فرض که تولیدکنندگان به طور ضمنی به داده‌های محصول و خدمات مرتبط دسترسی کامل دارند، به کاربران محصول اختصاص نمی‌دهد، درحالی‌که ممکن است لزوماً چنین نباشد. نویسنده پیشنهاد می‌کند که اعطای حق دسترسی به داده‌ها به تولیدکنندگان، نه تنها محیطی برابر بین طرفین تولیدکننده مشترک را بازیابی می‌کند، بلکه تولیدکنندگان را قادر می‌سازد تا اثرات شبکه مبتنی بر داده را ایجاد کنند که این امر ممکن است به نوآوری بیشتر در خدمات داده محور کمک کند. در پایان نویسنده توصیه می‌کند که ارزش اجتماعی داده‌ها را می‌توان با معرفی مفهوم فرسودگی متقابل حقوق داده‌ها، برای تولیدکنندگان و کاربران، در محل فروش محصول یا خدمات داده، به حداکثر رساند و آن را تنها مشروط به محدودیت‌های مربوط به حقوق از پیش موجود برای طرفین، مانند حقوق GDPR برای داده‌های شخصی یا اسرار تجاری برای داده‌های تجاری کرد.

۲. EU's 2022 Digital Markets Act



Pro- and anti-competitive provisions in the proposed European Union Data Act
 Bertin Martens
 Bruegel
 January 9, 2023

عنوان
 نویسنده
 مرکز مطالعاتی
 تاریخ انتشار

قانون هوش مصنوعی اتحادیه اروپا به سمت سطحی از استانداردهای هوش مصنوعی که وجود ندارند، می‌رود

قانون هوش مصنوعی پیشنهادی اتحادیه اروپا^۱ یک تلاش بلندپروازانه برای تنظیم توسعه و استقرار هوش مصنوعی در این اتحادیه است. با این حال، طبق جدیدترین مقاله منتشرشده در مؤسسه لافرا^۲ با وجود این که هنوز استانداردهای هوش مصنوعی وجود ندارد، قانون هوش مصنوعی به سمت اجرای آن می‌رود. در این مقاله آمده که قانون هوش مصنوعی به دنبال تنظیم طیف گسترده‌ای از برنامه‌های هوش مصنوعی، از جمله سیستم‌های هوش مصنوعی پرخطر است؛ اما تهیه‌کنندگان این قانون تعریف روشنی از آنچه «سیستم هوش مصنوعی» را تشکیل می‌دهد، ارائه نکرده‌اند. در نتیجه، این خطر وجود دارد که مقررات بسیار گسترده یا بسیار محدود باشد که این امر هم به‌طور بالقوه منجر به عواقب ناخواسته قابل توجهی می‌شود.



علاوه بر این، این مقاله استدلال می‌کند که قانون هوش مصنوعی فاقد یک رویکرد منسجم و روشن برای مقابله با پیچیدگی‌های سامانه‌های هوش مصنوعی است. به عنوان مثال، قانون مستلزم آن است که سامانه‌های هوش مصنوعی پرخطر تحت یک روش ارزیابی قرار بگیرند، اما مشخص نیست که این رویه چگونه انجام یا الزامی می‌شود. علاوه بر این، این قانون برای سامانه‌های هوش مصنوعی الزاماً شفافیت می‌خواهد، اما در مورد چگونگی دستیابی به شفافیت یا معنای آن در زمینه هوش مصنوعی راهنمایی ارائه نمی‌کند. یکی از نگرانی‌های اصلی مطرح‌شده در این مقاله این است که این قانون مانع نوآوری در بخش هوش مصنوعی می‌شود. با تعیین چنین الزامات سخت‌گیرانه‌ای برای توسعه و استقرار سیستم‌های هوش مصنوعی، این قانون ممکن است استارت‌آپ‌ها و دیگر نوآوران را از ورود به بازار منصرف کند. این امر می‌تواند در زمینه توانایی اروپا برای رقابت جهانی در بخش هوش مصنوعی پیامدهایی منفی داشته باشد.

نگرانی دیگری که در این مقاله مطرح می‌شود این است که قانون هوش مصنوعی می‌تواند منجر به «تخطی از مقررات» شود؛ زیرا کشورهای خارج از اتحادیه اروپا به دنبال جذب توسعه‌دهندگان و کاربران هوش مصنوعی با ارائه مقرراتی کمتر سخت‌گیرانه هستند. این امر می‌تواند منجر به وضعیتی شود که در آن توسعه و استقرار سامانه‌های هوش مصنوعی

۱. The European Union's (EU) proposed Artificial Intelligence Act (AI Act)

۲. Lawfare

در کشورهای مختلف، تابع استانداردهای بسیار متفاوتی باشد و به‌طور بالقوه منجر به مجموعه‌ای از مقررات می‌شود که توسعه سامانه‌های هوش مصنوعی قابل استقرار در سطح جهانی را دشوار می‌کند.

علی‌رغم این نگرانی‌ها، مقاله اشاره می‌کند که قانون هوش مصنوعی گامی مهم در جهت تنظیم سامانه‌های هوش مصنوعی است. این قانون خطرات بالقوه مرتبط با استقرار سامانه‌های هوش مصنوعی را تشخیص می‌دهد و به دنبال کاهش این خطرات از طریق ایجاد استانداردها و مقررات روشن است. با این حال، مقاله استدلال می‌کند که قانون هوش مصنوعی باید اصلاح شده و بهبود یابد تا از دستیابی به اهداف موردنظر خود بدون سرکوب نوآوری یا ایجاد پیامدهای ناخواسته اطمینان حاصل کند.

در پایان، مقاله مؤسسه لافر سؤالات مهمی را در مورد قانون پیشنهادی هوش مصنوعی اتحادیه اروپا مطرح می‌کند. با وجود این‌که این قانون نشان‌دهنده تلاش قابل‌توجهی برای تنظیم توسعه و استقرار سیستم‌های هوش مصنوعی است، اما همچنان نگرانی‌هایی در مورد تأثیر بالقوه آن بر نوآوری و رقابت جهانی بخش هوش مصنوعی اتحادیه اروپا وجود دارد. هم‌چنان‌که اتحادیه اروپا با اجرای قانون هوش مصنوعی پیش می‌رود، رسیدگی به این نگرانی‌ها و اطمینان از دستیابی این قانون به اهداف مورد نظر خود به‌گونه‌ای که نوآوری و رقابت را ارتقاء دهد و خطرات مرتبط با استقرار سامانه‌های هوش مصنوعی را کاهش دهد، مهم خواهد بود.



The EU's AI Act Is Barreling Toward AI Standards That Do Not Exist

Hadrien Pouget

Lawfare

January 12, 2023

عنوان

نویسنده

مرکز مطالعاتی

تاریخ انتشار

لزوم اعمال قانون برای ارزهای دیجیتال و بلاک چین

فناوری‌های مبتنی بر بلاک‌چین، فرصت‌های جدیدی را برای تراکنش‌های مالی و سایر معاملات بازکرده‌اند که رمز ارز شناخته شده‌ترین کاربرد آن است. ناشناس بودن نسبی ارزهای دیجیتال، آن را به ابزاری مناسب برای فعالیت‌های غیرقانونی تبدیل کرده است و لازم است مجریان قانون مهارت‌ها و شایستگی‌های جدیدی را برای بررسی چنین تراکنش‌هایی ایجاد کنند. برای رسیدگی به این چالش‌ها، محققان مؤسسه RAND و انجمن تحقیقات اجرایی پلیس کارگاهی^۱ جلساتی را در حمایت از مؤسسه ملی عدالت^۲ برگزار کردند. این جلسات ۲۴ الزام تحقیق و توسعه‌ای را شناسایی و اولویت‌بندی کرد که اگر روی آن‌ها سرمایه‌گذاری شود، توانایی اجرای قانون برای انطباق با این تغییرات اجتماعی بهبود می‌یابد. این الزام‌ها که بدان تأکید شده است حول موضوعاتی مانند:

- سیاست‌هایی برای مدیریت کلید دیجیتال^۳
- منابعی برای آموزش اجرای قانون در مورد بلاک‌چین و ارزهای دیجیتال
- ابزارهایی برای تحقیقات مربوط به ارزهای دیجیتال است.

این گزارش خاطرنشان می‌کند که آموزش‌های کافی در خصوص بلاک‌چین و ارزهای دیجیتال ویژه مجریان قانون و متخصصان برای پاسخگویی نیاز به آموزش عدالت‌خواهان وجود ندارد. علاوه بر این، هرکسی که یک کلید دیجیتال در اختیار دارد، می‌تواند ارز دیجیتال را منتقل کند و این امر، تصاحب و مصادره دارایی‌ها را برای مجریان قانون دشوار می‌کند. دارایی‌های رمزنگاری توقیف شده نیز می‌توانند به کیف پولی دیجیتالی با مالکیتی ناشناخته منتقل شوند و فرصت‌هایی را برای سوءاستفاده ایجاد کنند. این گزارش همچنین فقدان تخصص در تمام جنبه‌های فناوری‌های بلاک‌چین و ارزهای دیجیتال در سراسر سیستم قضایی و دشواری در همگام شدن با تکامل سریع این فناوری‌ها را یادآور می‌شود.

این گزارش برای رسیدگی به این چالش‌ها توصیه می‌کند که بهترین سیاست‌ها و رویه‌ها برای ایمن‌سازی دارایی‌های رمزنگاری شده و به حداقل رساندن فرصت‌ها برای سوءاستفاده از ارزهای دیجیتال شناسایی شود. علاوه بر این، این گزارش فهرست‌نویسی و انتشار منابع آموزشی موجود، توسعه سامانه‌های اشتراک‌گذاری منطقه‌ای یا ملی برای اطلاعات عملی و انجام تحقیقات برای بررسی تعادل مهارت‌ها و تخصص مورد نیاز سازمان‌های مجری قانون را پیشنهاد می‌کند. در نهایت، این گزارش همکاری با نهادهای فدرال، ایالتی، محلی و خصوصی را برای در دسترس قرار دادن منابع مناسب ردیابی ارزهای دیجیتال و ارزیابی هزینه‌ها و مزایای ایجاد یک اتاق تسویه بخش خصوصی برای هماهنگی تلاش‌ها، پیشنهاد می‌کند.

۱. Police Executive Research Forum
 ۲. National Institute of Justice
 ۳. Digital Key

یافته‌های کلیدی این گزارش عبارت‌اند از:

- فقدان آموزش برای مجریان قانون درمکرد ارزهای دیجیتال و بلاک-چین.
- وابستگی این دارایی‌ها به یک رمز و امکان سوءاستفاده هر فردی که به این رمز دسترسی پیدا کند.
- همچنین در این گزارش پیشنهادهای زیر مطرح شده است:
- شناسایی خط‌مشی‌ها و رویه‌های بهتر برای ایمن‌سازی سریع دارایی‌های ارزهای دیجیتال در طول تحقیقات توسط بازرسان.
- شناسایی خط‌مشی‌ها و رویه‌های بهتر برای به حداقل رساندن فرصت‌های سوءاستفاده از ارزهای دیجیتال.
- تهیه و انتشار منابع آموزشی برای افزایش مهارت مجریان قانون جهت پیش‌گیری سوءاستفاده از رمز ارزها.



Cryptocurrency and Blockchain Needs for Law Enforcement
,Dulani Woods, John S. Hollywood, Jeremy D. Barnum, Danielle Fenimore, Michael J. D. Vermeer
Brian A. Jackson
RAND
January, 2023

عنوان
نویسنده

مرکز مطالعاتی
تاریخ انتشار



نیمه‌هایها

چشم انداز هند در رقابت جهانی تولید نیمه‌هادی‌ها

پژوهشگران شورای روابط خارجی (CFR) در جدیدترین مقاله خود درباره تلاش‌های هند برای ایجاد صنعت نیمه‌هادی داخلی و رقابت با سایر کشورها، عملکرد این کشور را مورد بحث قرار می‌دهند. آن‌ها خاطرنشان می‌کنند با این وجود که هند مدتی طولانی مصرف‌کننده عمده نیمه‌هادی‌ها بوده، اما از نظر توانایی‌های تولید داخلی از سایر کشورها عقب مانده است. با این حال، آن‌ها استدلال می‌کنند که هند با توجه به بازار بزرگ و رو به رشد خود برای صنایع الکترونیک و دارا بودن مجموعه‌ای از مهندسان و دانشمندان بسیار ماهر، پتانسیل تبدیل شدن به یک بازیگر اصلی در صنعت نیمه‌هادی را دارد. بر اساس توضیحات این پژوهشگران، دولت هند اقداماتی را برای حمایت از توسعه صنعت نیمه‌هادی داخلی انجام داده است؛ برای مثال طرح تشویقی مرتبط با تولید (PLI) که اخیراً اعلام عمومی شده است. بر همین اساس، آن‌ها بر این باورند که هدف هند برای ایجاد یک اکوسیستم نیمه‌هادی موفق اخیراً به نقطه عطف جدیدی رسیده است، زیرا ائتلاف بین‌المللی نیمه‌هادی مستقر در اسرائیل اعلام کرده که قصد دارد ساخت اولین کارخانه تولید نیمه‌هادی را در فوریه ۲۰۲۳ در کشور هند آغاز کند. برای این منظور شرکت هندی «Vedanta» و سازنده تایوانی «FoxConn» نیز اخیراً ۱۹ میلیارد دلار در ساخت نیمه‌هادی سرمایه‌گذاری کردند. برای ساخت کارخانه‌های تولید نیمه‌هادی دو سال زمان لازم است. هند در تولید داخلی نیمه‌هادی‌ها سرمایه‌گذاری کرده است تا ضمن تأمین مصرف داخلی نیمه‌هادی، به یکی از بارزترین فناوری‌های جهان دست پیدا کند.

از سوی دیگر، این مقاله چالش‌هایی را که هند در رقابت با بازیگران مطرحی مانند چین، ایالات متحده و تایوان با آن مواجه خواهد شد را نیز بررسی می‌کند. این چالش‌ها شامل کمبود زیرساخت و موانع نظارتی و هزینه‌های بالا و پیچیدگی‌های فنی ساخت نیمه‌هادی‌ها است. با این حال، آن‌ها خاطرنشان می‌کنند که مزایای هند از نظر سرمایه انسانی و پتانسیل بازار می‌تواند کمک کند تا بر این چالش‌ها غلبه کرده و به‌عنوان یک بازیگر مهم در صنعت نیمه‌هادی جهانی ظاهر شود.



۱. Production Linked Incentive (PLI)



India's Prospects in the Global Semiconductor Manufacturing Race
Srishti Khemka, Guest Contributor
CFR
December 21, 2022

عنوان
نویسنده
مرکز مطالعاتی
تاریخ انتشار

جنگ بر سر بحرانی‌ترین فناوری جهان

شورای روابط خارجی آمریکا به‌تازگی گفتگویی با کریس میلر، یک مقام سابق دولت ایالات‌متحده و نویسنده کتاب «جنگ تراشه‌ها» انجام داده است. این گفتگو بر رقابت استراتژیک بین ایالات‌متحده و چین بر سر فناوری‌های حیاتی مانند هوش مصنوعی، نیمه‌هادی‌ها و محاسبات کوانتومی متمرکز است. میلر در این گفتگو استدلال می‌کند که رقابت این دو کشور بر سر این فناوری‌ها احتمالاً ویژگی خاص قرن بیست و یکم است. وی خاطرنشان می‌کند که این دو کشور اساساً رویکردهای متفاوتی در زمینه نوآوری و توسعه فناوری دارند، به‌گونه‌ای که چین بر تلاش‌های دولتی تأکید می‌کند و ایالات‌متحده بیشتر بر مکانیسم‌های مبتنی بر بازار تکیه دارد. میلر در مورد پیامدهای این رقابت استراتژیک برای امنیت ملی ایالات‌متحده و اقتصاد جهانی صحبت می‌کند. او استدلال می‌کند که ایالات‌متحده در حفظ برتری فناوری خود با چالش‌های مهمی مواجه است، از جمله نیاز به رسیدگی به آسیب‌پذیری‌های زنجیره تأمین و جذب و حفظ استعداد‌های برتر در علم. به‌طورکلی، میلر بر اهمیت حیاتی فناوری در شکل دادن به پویایی قدرت جهانی در قرن بیست‌ویکم تأکید می‌کند. ایالات‌متحده با درک ماهیت این رقابت و توسعه استراتژی‌های مؤثر برای آن، می‌تواند به تضمین تداوم موفقیت اقتصادی و استراتژیک خود در سال‌های آینده کمک کند. برخی دیگر از مهم‌ترین سؤالاتی که میلر در این گفتگو به آن‌ها پاسخ می‌دهد، به شرح ذیل است:

- چرا تراشه‌ها تا این اندازه مهم هستند و چه اتفاقی سبب تبدیل شدن آن‌ها به یک مسئله جهانی شده است؟
- با توجه به انحصار تایوان در تولید نیمه‌هادی، در صورت تحریم توسط تایوان چه عواقبی در انتظار آمریکا است؟
- آیا استقلال آمریکا از تایوان سیاست صحیحی است؟
- علی‌رغم اینکه چین صدها میلیارد دلار به شرکت‌های داخلی برای تولید نیمه‌هادی داده است، چرا این تلاش‌ها تا حد زیادی شکست خورده است؟



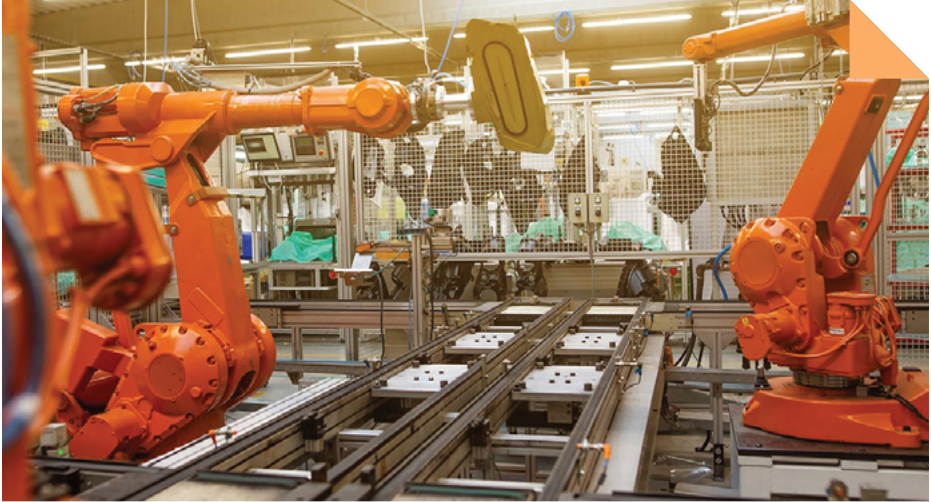
The War Over the World's Most Critical Technology: A Conversation with Chris Miller
David Sacks, Chris Miller
CFR
January 3, 2023

عنوان
نویسنده
مرکز مطالعاتی
تاریخ انتشار





حکمرانی سایبری



دستور کار فناوری آمریکا در سال ۲۰۲۳

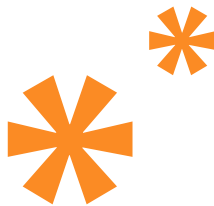
کلود بارفیلد، در مقاله اخیر خود در مورد آینده فناوری و نوآوری صحبت می‌کند. طبق استدلال بارفیلد با اینکه نوآوری در بخش فناوری بدون شک مزایای اقتصادی متعددی به همراه داشته، چالش‌های مهمی را نیز برای سیاست‌گذاران ایجاد کرده است. او پیش‌بینی می‌کند در سال آینده چندین موضوع کلیدی، گفتگو پیرامون فناوری و نوآوری را شکل خواهند داد؛ از جمله بحث در مورد مقررات شرکت‌های بزرگ فناوری، تنش مداوم بین حریم خصوصی و نگرانی‌های امنیتی و این سؤال که آیا ایالات متحده می‌تواند موقعیت خود را به عنوان رهبر جهانی نوآوری فن‌آورانه حفظ کند یا خیر.

بارفیلد ادعا می‌کند که مسئله چگونگی تنظیم فناوری‌های بزرگ در سال ۲۰۲۳ یک موضوع بحث‌برانگیز خواهد بود، زیرا سیاست‌گذاران و عموم مردم همچنان با نگرانی‌هایی در خصوص حریم خصوصی داده‌ها، رقابت و آزادی بیان دست‌وپنجه نرم می‌کنند. او پیشنهاد می‌کند که سیاست‌گذاران باید راهی بیابند تا مزایای نوآوری‌های این شرکت‌ها را با نیاز به نظارت و مقررات مؤثر متعادل کنند. علاوه بر این، بارفیلد بر اهمیت پرداختن به پیامدهای بالقوه فناوری‌های نوظهور برای امنیت ملی، مانند هوش مصنوعی و شبکه‌های 5G، تأکید می‌کند؛ چراکه ایالات متحده علی‌رغم حفظ برتری فناوری خود باید ملاحظات امنیت ملی را نیز در نظر بگیرد.

به‌طورکلی، مقاله بارفیلد دیدگاه ارزشمندی در مورد مسائل عمده‌ای که احتمالاً چشم‌انداز فناوری و نوآوری را در سال ۲۰۲۳ شکل می‌دهد، ارائه کرده است. تأکید او بر نیاز سیاست‌گذاران به ایجاد تعادل به هنگام بین مزایای پیشرفت فناوری و خطرات ناشی از آن است، زیرا بحث‌های مربوط به حریم خصوصی، امنیت و مقررات همچنان بر گفتمان عمومی حاکم است. به‌این‌ترتیب، تحلیل او چارچوب مفیدی را برای سیاست‌گذاران و رهبران حوزه فناوری فراهم می‌کند که می‌خواهند این مسیر پیچیده و به‌سرعت در حال تحول را هدایت کنند.

برخی از محورهایی که انتظار می‌رود در سال ۲۰۲۳ توسط دولت آمریکا دنبال شود، به شرح ذیل است:

- اولین محور توجه به تجارت دیجیتال است. دولت بایدن به‌طور مداوم از سیاست‌های خود در باب اقتصاد دیجیتال به‌عنوان اولویت اول برای آمریکا یاد می‌کند. درحالی‌که برای ساختن یک تجارت دیجیتال موفق از توافق نامه آمریکا-مکزیک-کانادا اجتناب می‌کند.
- دومین محور توجه به روابط تجاری و فناوری آمریکا و اتحادیه اروپا است. بعد از رفتن ترامپ اروپا تصور می‌کرد که روابط فناوری آنان بهبود می‌یابد، درحالی‌که بایدن همچنان منفعلانه عمل کرده و از ظرفیت شورای تجارت و فناوری آمریکا و اتحادیه اروپا (TTC) بهره نمی‌گیرد.
- علی‌رغم کنترل‌های صادرات فناوری توسط بایدن، همچنان شرکت هوآوی به فعالیت در اروپا ادامه می‌دهد. چگونگی چشم‌انداز فعالیت این شرکت در سال ۲۰۲۳ محور دیگر مورد بحث است.
- دستیابی به توافق در مورد قانون کاهش تورم یکی از چالش‌برانگیزترین و احتمالاً یکی از حل‌نشده‌ترین مسائل فناوری و تجارت روی میز مذاکره ایالات متحده و اتحادیه اروپا است که باید در سال ۲۰۲۳ حل شود.



Looking Ahead to 2023 with Claude Barfield
 Claude Barfield
 AEI
 January 3, 2023

عنوان
 نویسنده
 مرکز مطالعاتی
 تاریخ انتشار

تغییر رویکرد دولت‌های غربی از اینترنت یکپارچه به اینترنت تکه‌تکه شده

شورای روابط خارجی در این مقاله، بحث‌های جاری پیرامون حکمرانی سایبری و نقش دولت‌های غربی در ترویج اینترنت آزاد و رایگان را مورد بررسی قرار می‌دهد. نویسندگان استدلال می‌کنند درحالی‌که این دولت‌ها مدت‌هاست از اهمیت اینترنت باز حمایت کرده‌اند، اقدامات آن‌ها اغلب در تضاد با این لفاظی بوده است.

در این مقاله چندین نمونه از جمله تصمیم اخیر ایالات متحده برای خروج از فراخوان اعتماد و امنیت در فضای سایبری پاریس، به‌عنوان شاهی بر تناقض بین سخنان و اقدامات دولت‌های غربی در مورد حکمرانی اینترنت ذکر شده است. نویسندگان خاطرنشان می‌کنند با وجود اینکه فراخوان پاریس بر اهمیت ترویج اینترنت رایگان و امن تأکید می‌کرد، خروج ایالات متحده این تلاش‌ها را تضعیف می‌کند.

این مقاله پیامدهای گسترده‌تر این قطع ارتباط برای حاکمیت جهانی اینترنت را نیز بررسی می‌کند؛ از جمله پتانسیل سایر کشورها برای اتخاذ سیاست‌های محدودکننده‌تر و کاهش اعتماد به تلاش‌های غرب برای ترویج اینترنت باز. آن‌ها توضیح می‌دهند که برای سال‌ها کارشناسان به تنش‌های ذاتی در شعار دموکراسی‌های لیبرال برای اینترنت «باز، رایگان و ایمن» اشاره کرده‌اند. به همین دلیل، اخیراً یک کارگروه در شورای روابط خارجی خواستار بازبینی سیاست خارجی دیجیتال ایالات متحده بر این اساس شده است که «دوران اینترنت جهانی به پایان رسیده است». با این وجود ایالات متحده و سایر دولت‌های غربی که شعارهای اینترنت باز و آزاد و یکپارچه می‌دادند در IGF امسال از رویکردهای سیاستی که منجر به پراکندگی اینترنت می‌شود، حمایت کردند. اکنون دولت‌های غربی و سایرین علاقه‌مند به اینترنت آزاد و باز باید تبیین کنند که چه شکالی از پراکندگی در اینترنت قابل قبول است. نویسندگان در پایان از دولت‌های غربی می‌خواهند تا اقدامات خود را با تعهدات از پیش اعلام شده خود نسبت به اینترنت آزاد و رایگان، از جمله حمایت از تلاش‌ها برای ارتقای حقوق دیجیتال و مبارزه با سانسور، هماهنگ کنند.

به‌طور کلی این مقاله، ماهیت پیچیده و اغلب متناقض حکمرانی سایبری در دنیای امروز را برجسته می‌کند. با اینکه دولت‌های غربی نقش مهمی در ترویج اینترنت آزاد و باز داشته‌اند، اگر می‌خواهند اعتبار و اثربخشی در این حوزه حیاتی را حفظ کنند، باید بیشتر تلاش کرده و از همخوانی اقدامات و شعارهایشان اطمینان حاصل کنند.

۱. Paris Call for Trust and Security in Cyberspace

Internet Governance Doublepeak: Western Governments and the Open Internet

Zoe Hawkins, Guest Contributor

CFR

January 4, 2023

عنوان

نویسنده

مرکز مطالعاتی

تاریخ انتشار



پیامد جمع‌آوری و انتشار داده‌ها بر حریم خصوصی

مقاله «داده‌ها طلای جدید هستند، اما ممکن است دموکراسی و کرامت را تهدید کنند» از شورای روابط خارجی به بررسی خطرات و چالش‌های بالقوه افزایش تلقی داده‌ها به‌عنوان یک کالای ارزشمند در عصر دیجیتال امروزی می‌پردازد. این مقاله برداشتی از گفتگو با پروفیسور سیترون^۱ پیرامون کتاب جدید خود درباره پیامدهای جمع‌آوری و انتشار داده‌های شخصی است. نویسندگان استدلال می‌کنند درحالی‌که داده‌ها پتانسیل ایجاد نوآوری و رشد اقتصادی را دارند، خطرات قابل‌توجهی برای حریم خصوصی افراد، دموکراسی و کرامت انسانی نیز به همراه دارند. او هشدار می‌دهد تهدیداتی که فناوری برای حریم خصوصی ایجاد می‌کند، فراتر از بیان فردی است و همچنین تهدیدی برای امنیت ملی به حساب می‌آید. دیپ‌فیک‌ها، تغییر صوت‌های ضبط‌شده یا یک ویدیوی جعلی، می‌توانند نتایج یک انتخابات را تغییر دهند. او با ذکر مثالی، می‌گوید که تصور کنید ویدیوی قانع‌کننده‌ای از رئیس‌جمهور بایدن که به تقلب در انتخابات ایالات متحده اعتراف می‌کند یا یک سخنرانی که شبیه به اعلان جنگ است در رسانه‌های اجتماعی منتشر شود. این موارد چه آثاری برای امنیت ملی در پی خواهد داشت؟

این مقاله چندین موضوع کلیدی در خصوص کالایی‌سازی داده‌ها را بررسی می‌کند؛ از جمله جمع‌آوری و استفاده از داده‌های شخصی توسط شرکت‌های فناوری، تأثیر تصمیم‌گیری مبتنی بر داده بر نابرابری اجتماعی و خطرات نظارت و سانسور. نویسندگان همچنین خاطرنشان می‌سازد که اهمیت روزافزون داده‌ها منجر به افزایش رقابت ژئوپلیتیکی شده است، به طوری که دولت‌ها و شرکت‌ها برای کنترل جریان داده‌ها و دسترسی به مجموعه داده‌های باارزش رقابت می‌کنند. نویسندگان بر نیاز فوری به شفافیت و پاسخگویی بیشتر در مورد جمع‌آوری و استفاده از داده‌ها و همچنین حمایت‌های قانونی بیشتر از حریم خصوصی افراد و حقوق بشر، تأکید دارد. نویسندگان استدلال می‌کنند که پرداختن به این موضوعات نیازمند رویکردی چندوجهی است که شامل همکاری بین دولت‌ها، صنعت، جامعه مدنی و افراد است تا از اشتراک‌گذاری عادلانه مزایای نوآوری مبتنی بر داده‌ها و کاهش خطرات دموکراسی و کرامت انسانی اطمینان حاصل شود.

به‌طورکلی، این مقاله یک نمای جامع از خطرات و چالش‌های مرتبط با اهمیت روزافزون داده‌ها در عصر دیجیتال امروزی ارائه می‌دهد و نیاز به رویکردی دقیق‌تر و جامع‌تر برای حکمرانی بر داده‌ها را برجسته می‌کند که حریم خصوصی افراد، ارزش‌های دموکراتیک و کرامت انسانی را در اولویت قرار داده و درعین حال نوآوری و رشد اقتصادی را نیز ارتقا می‌دهد.

۱. Citron



Data is the New Gold, But May Threaten Democracy and Dignity
Catherine Powell, Alexandra Dent, Guest Contributors
CFR
January 5, 2023

عنوان
نویسنده
مرکز مطالعاتی
تاریخ انتشار



تأخیر در اجرای سیاست کنترل صادرات فناوری به چین

در این مقاله که توسط بنیاد هریتیج منتشر شده است، نویسندگان استدلال می‌کنند که کنترل صادرات فناوری به چین مدت‌ها به تعویق افتاده و اجرا و نظارت مؤثر برای جلوگیری از گسترش فناوری‌های حساس به کشورهای متخاصم حیاتی است. نویسندگان تأکید می‌کنند که چین مدت‌هاست که از سیستم اقتصاد جهانی برای دستیابی به فناوری‌های حساس و مالکیت معنوی از راه‌های قانونی و غیرقانونی سوءاستفاده کرده و این اقدامات امنیت ملی و رقابت اقتصادی را تضعیف نموده است. نویسندگان تلاش‌های اخیر ایالات متحده برای رسیدگی به این چالش‌ها را مورد بحث قرار می‌دهند؛ از جمله قانون اصلاح کنترل صادرات مصوب سال ۲۰۱۸ و «فهرست نهادهای دفتر صنعت و امنیت وزارت بازرگانی»^۱ که هر دوی آن‌ها به شناسایی شرکت‌ها و افرادی می‌پردازند که خطری برای کشور ایجاد کرده و محدودیت‌هایی را برای دسترسی آن‌ها به فناوری ایالات متحده اعمال می‌کنند. نویسندگان همچنین بر اهمیت همکاری بین‌المللی در پرداختن به این چالش‌ها، از جمله تلاش برای ایجاد استانداردهای مشترک کنترل صادرات و تقویت رژیم جهانی منع اشاعه تأکید می‌کنند.

آخرین دوره از کنترل‌های صادراتی ایالات متحده شامل تراشه‌های نیمه‌هادی و نیروی انسانی به چین می‌شود. این محدودیت در صادرات برای تضمین رهبری آمریکا در نیمه‌هادی‌ها و حفظ مزیت اقتصادی ایالات متحده است. ثمره دیگر آن محدود کردن پیشرفت چین در توسعه فناوری و جلوگیری از به خطر افتادن امنیت ملی آمریکا است. در نتیجه ضروری است که این کنترل‌ها به درستی اجرا شوند. در همین راستا، دولت ترامپ کنترل صادرات قابل‌توجهی را برای انتقال و فروش فناوری نیمه‌هادی به بزرگ‌ترین سازنده تراشه چین، شرکت بین‌المللی تولید نیمه‌هادی SMIC اعمال کرد. اقدامات کنترل صادرات جدید اعلام شده

۱. Export Control Reform Act of 2018

۲. The Commerce Department's Bureau of Industry and Security (BIS) "Entity List"



در ۷ اکتبر شامل محدودیت‌های جدید در دسترسی چین به دستگاه‌های ساخت نیمه‌هادی، طراحی، متخصصان و تجهیزات برای برنامه‌های کاربردی ابررایانه و هوش مصنوعی است.

به‌طورکلی این مقاله مروری جامع از چالش‌های ناشی از دستیابی چین به فناوری‌های حساس و اهمیت سیاست‌های کنترل صادرات مؤثر در پرداختن به این چالش‌ها را ارائه می‌دهد. نویسندگان در سرتاسر این مقاله بر لزوم اجرا و نظارت مؤثر بر سیاست‌های کنترل صادرات تأکید کرده و استدلال می‌کنند که اجرای ضعیف و نظارت ناکافی می‌تواند اثربخشی سیاست‌هایی که به‌خوبی طراحی شده‌اند را نیز تضعیف کند. تأکید نویسندگان بر اهمیت اجرا و نظارت، ضرورت اتخاذ رویکردی جامع و استراتژیک به‌منظور کنترل صادرات برای سیاست‌گذاران را با در نظر گرفتن ملاحظات اقتصادی و امنیت ملی برجسته می‌کند.



Chinese Exports Controls Overdue: Implementation and Oversight Is Key
Min-Hua Chiang, Erin Walsh
Heritage
January 5, 2023

عنوان
نویسنده
مرکز مطالعاتی
تاریخ انتشار

برطرف کردن نابرابری اجتماعی با جمع‌آوری بهتر داده‌ها

در اقتصاد دیجیتال امروزی، یکی از موانع مهم در برقراری برابری فرصت‌ها، شکاف داده‌ها است که به معنی برخورداری برخی مردم از داده‌ها و عدم دسترسی گروهی دیگر به داده‌ها و نیز نابرابری‌های اجتماعی و اقتصادی است که از عدم جمع‌آوری و استفاده از داده‌ها ناشی می‌شود. کاهش شکاف داده‌ها باید یک اولویت سیاستی در ایالات متحده باشد تا رشد قوی و عادلانه در اقتصاد دیجیتال ایجاد کند که در این یادداشت نویسنده به تفصیل این ایده می‌پردازد.

در این مقاله، نویسنده استدلال می‌کند که جمع‌آوری بهتر داده‌ها می‌تواند به کاهش نابرابری‌های دیجیتالی منجر شود و از طریق توانمندسازی سیاست‌گذاران برای شناسایی و رفع شکاف‌ها به مسئله دسترسی به فناوری‌های دیجیتال و اینترنت کمک کند. نویسنده خاطرنشان می‌کند با وجود اینکه فناوری‌های دیجیتال از بسیاری جهات، از جمله با فراهم کردن دسترسی به آموزش، مراقبت‌های بهداشتی و فرصت‌های شغلی، پتانسیل بهبود زندگی مردم را دارند، همه افراد به این فناوری‌ها دسترسی برابر ندارند. این امر به‌ویژه برای افرادی که در مناطق روستایی یا کم‌درآمد زندگی می‌کنند یا دارای معلولیت بوده یا متعلق به سایر گروه‌های حاشیه‌ای هستند، صادق است.

نویسنده پیشنهاد می‌کند که جمع‌آوری بهتر داده‌ها می‌تواند به شناسایی شکاف دسترسی کمک کرده و سیاست‌گذاران را قادر سازد تا مداخلات هدفمندی برای رفع آن‌ها توسعه دهند. به‌عنوان مثال، با جمع‌آوری داده‌ها در مورد دسترسی به پهنای باند و سرعت اینترنت، سیاست‌گذاران می‌توانند مناطقی را شناسایی کنند که فاقد دسترسی به اینترنت پرسرعت است و بودجه مستقیم برای گسترش زیرساخت‌های پهنای باند در آن مناطق اختصاص دهند. همچنین با جمع‌آوری داده‌ها در مورد استفاده از فناوری‌های دیجیتال در آموزش و مراقبت‌های بهداشتی، سیاست‌گذاران می‌توانند گروه‌هایی را شناسایی کنند که از خدمات کمتری برخوردار هستند و برنامه‌هایی را برای افزایش دسترسی به این خدمات توسعه دهند.

به‌طور کلی، جمع‌آوری بهتر داده‌ها برای کاهش نابرابری‌های دیجیتال و اطمینان از دسترسی همه افراد به فرصت‌هایی که فناوری‌های دیجیتال ارائه می‌دهند، ضروری است. نویسنده از سیاست‌گذاران می‌خواهد که در تلاش‌های خود برای افزایش شمول دیجیتال و کاهش نابرابری، جمع‌آوری و تجزیه و تحلیل داده‌ها را در اولویت قرار دهند.

Better Data Collection Will Reduce Digital Inequalities
Gillian Diebold
ITIF
January 2, 2023

عنوان
نویسنده
مرکز مطالعاتی
تاریخ انتشار



استارت‌آپ‌های فناوری هند

این مقاله نمایی کلی از وضعیت فعلی استارت‌آپ‌های فناوری هند را ارائه می‌دهد و موفقیت‌ها و چالش‌های آن‌ها را برجسته می‌کند. دولت هند بر استارت‌آپ‌های فناوری خود به‌عنوان بخش مهمی از سیاست توسعه اقتصادی تأکید و از آن استقبال می‌کند. نخست‌وزیر هند اخیراً اشاره کرده است که تعداد «یونیکورن‌های» هندی (شرکت‌های استارت‌آپ فناوری با ارزش ۱ میلیارد دلار یا بیشتر) از سال ۲۰۲۱ دو برابر شده است. از سوی دیگر اگرچه هند به‌عنوان سومین اکوسیستم بزرگ برای استارت‌آپ‌ها ظاهر شده است، اما تأمین مالی این استارت‌آپ‌ها در حال تبدیل شدن به یک معضل فراگیر است. به‌طوری‌که تعداد یونیکورن‌ها در سال ۲۰۲۲ به نصف کاهش یافته است. استارت‌آپ‌های فناوری هند در طول همه‌گیری دو ساله کرونا بسیار خوب عمل کردند. استارت‌آپ‌های فناوری آنلاین با افزایش چشمگیر تعاملات اداری دورکاری، مشاوره آنلاین برای خدمات مختلف به‌ویژه مراقبت‌های بهداشتی، کلاس‌های آنلاین در مدارس و سایر مراکز آموزشی و نیز سایر خدمات در بستری‌های آنلاین روبرو شده، درحالی‌که برخی دیگر از استارت‌آپ‌ها با مشکلات متعددی مواجه شدند.

در طول دوران کرونا، ابزارهای فناوری و ارتباطات الکترونیکی با استفاده از پلتفرم‌های مجازی، سیستم پرداخت دیجیتال و مشاوره‌های ویدیویی محبوب شدند، اما با توجه به اینکه همه‌گیری کرونا اکنون نسبتاً تحت کنترل است و مردم به زندگی عادی بازمی‌گردند، آینده استارت‌آپ‌های هندی که خدمات آنلاین ارائه می‌کنند رو به وخامت است. با توجه به گزارش‌های اخیر رسانه‌ها، آینده این شرکت‌های استارت‌آپ فناوری چندان روشن نیست. سرمایه‌ها در حال کاهش است و همه استارت‌آپ‌ها نمی‌توانند به فعالیت خود ادامه دهند. علاوه‌براین، مسائلی مانند حمله روسیه به اوکراین، افزایش نرخ تورم جهانی و ترس از رکود اقتصادی مزید بر علت بوده است. کمبود سرمایه که برای استارت‌آپ‌ها مسئله‌ای حیاتی است، منجر به اقداماتی برای کاهش هزینه‌ها مانند اخراج کارکنان، ادغام بخش‌های مختلف و حتی تعطیلی کامل برخی از آن‌ها شده است. به‌گونه‌ای که در سال ۲۰۲۲ هشت استارت‌آپ کار خود را تعطیل کرده‌اند.

به‌طورکلی، این مقاله نشان می‌دهد درحالی‌که استارت‌آپ‌های فناوری هند در سال‌های اخیر پیشرفت قابل‌توجهی داشته‌اند، هنوز چالش‌هایی وجود دارد که باید به آن‌ها پرداخته شود؛ از جمله بهبود محیط نظارتی، جذب سرمایه‌گذاری خارجی بیشتر و حمایت از استارت‌آپ‌ها در بخش‌هایی که به‌شدت تحت تأثیر همه‌گیری کرونا قرار گرفته‌اند.



Indian tech startups: A mixed picture
Rajeswari Pillai Rajagopalan
ORFonline
December 27, 2022

عنوان
نویسنده
مرکز مطالعاتی
تاریخ انتشار

بررسی تعاریف و پیامدهای حق حاکمیت سایبری

این مقاله به بررسی مفهوم حاکمیت سایبری می‌پردازد؛ این ایده که دولت‌ها حق دارند بر جریان اطلاعات و داده‌ها در داخل مرزهای خود حکمرانی کنند. این مفهوم برای درک عصر دیجیتال بسیار مهم است، زیرا بر مسائلی مانند حکمرانی اینترنت، حریم خصوصی آنلاین و امنیت ملی اثرگذار است. نویسنده پیش از پرداختن به مفهوم حق حاکمیت سایبری، تاریخچه مختصری از تحول فضای سایبری و رابطه آن با حقوق بین‌الملل و دیپلماسی ارائه می‌کند. با وجود اینکه ایده فضای مجازی بدون مرز و مشترک جهانی رایج شده، پرواضح است که دولت‌ها به دنبال اعمال کنترل بر سهم خود از اینترنت هستند. این امر منجر به افزایش اشکال مختلف حمایت‌گرایی دیجیتال، از جمله توسعه فایروال‌های ملی، سیاست‌های محلی‌سازی داده‌ها و سایر اقداماتی شده است که جریان داده‌های فرامرزی را محدود می‌کند. در حالی که برخی از کشورها مانند ایالات متحده از جریان آزاد اطلاعات حمایت می‌کنند، برخی دیگر مانند چین به‌طور پیش‌فرض جریان را برای شهروندان خود محدود می‌کنند که منجر به تکه‌تکه شدن اینترنت می‌شود.

فضای مجازی برخلاف سایر قلمروهای مصنوع انسان که ایستا هستند، روزبه‌روز به گسترش و نوآوری خود ادامه می‌دهد. همچنین برخلاف سایر فناوری‌هایی که توسعه آن‌ها توسط سیاست پیش می‌رود، در اینجا این فناوری است که تصمیم‌گیری‌های سیاستی را هدایت می‌کند. این ویژگی‌ها حکمرانی فضای مجازی را پیچیده می‌کند و منجر به تقابل بین دولت‌ها و سایر ذی‌نفعان می‌شود. چنین رویارویی‌هایی منجر به تشدید مرزبندی در فضای مجازی شده است. حکمرانی سایبری و درک آن توسط قدرت‌های جهانی، نیاز به ارزیابی دقیق‌تری دارد.

این مقاله ابهام موجود در مفهوم «حق حاکمیت سایبری» و کاربردهای آن را بررسی کرده و بیان می‌کند که چگونه حق حاکمیت سایبری به‌عنوان یک مفهوم با ظهور فرصت‌ها و تهدیدها در فضای سایبری تغییر کرده است. نویسنده بر حوادثی که به‌عنوان کاتالیزور حق حاکمیت سایبری برای دولت‌ها عمل کرده‌اند، تأکید و پیامدهای آن را بررسی می‌کند. این مقاله با این استدلال به پایان می‌رسد که مفهوم حاکمیت سایبری به شکل دهی آینده فضای سایبری ادامه می‌دهد و برای سیاست‌گذاران و محققان مهم است که در بحثی قوی پیرامون پیامدهای آن شرکت کنند. این امر هم نیاز به افزایش همکاری و گفت‌وگوی بین‌المللی برای اطمینان از باز، امن و قابل‌دسترس بودن اینترنت برای همه کاربران و همچنین احترام به منافع مشروع دولت‌ها برای حکمرانی بر جریان اطلاعات در داخل مرزهایشان را برجسته می‌کند.



بازارهای دیجیتال پرمخاطره ژاپن

همه‌گیری کرونا باعث تحول دیجیتال در سراسر ژاپن شده و فرصت‌های جدیدی را برای مشاغل و مصرف‌کنندگان به طور یکسان ایجاد کرده است. با این حال، بازارهای دیجیتال ژاپن با چالش‌هایی روبه‌رو بوده و دستخوش تغییرات مهمی هستند که نیازمند توجه فوری سیاست‌گذاران است. این چالش‌ها شامل افزایش رقابت از سوی غول‌های فناوری خارجی، نگرانی در مورد حریم خصوصی و امنیت داده‌ها و نیاز به مقررات کارآمدتر است. گروه تجارت منصفانه ژاپن به دنبال ایجاد تغییراتی است که رویه‌های تجاری ناعادلانه توسط پلتفرم‌های دیجیتال را ارزیابی کند. این آژانس در حال حاضر مسئول اجرای قوانین رقابت در این کشور و ترویج شیوه‌های تجارت منصفانه است. در سال ۲۰۲۰ این نهاد یک کارگروه ویژه ایجاد کرد تا به طور خاص بر مسائل دیجیتال تمرکز کند. این امر ممکن است منجر به اشتراک‌گذاری اجباری داده توسط پلتفرم‌ها با اشخاص ثالث شود که چندین خطر بالقوه مانند آسیب به حریم خصوصی و امنیت افراد و نیز افزایش هزینه‌های بالقوه انتقال داده به کشور ثالث را با خود به همراه دارد.

یکی دیگر از بزرگ‌ترین چالش‌هایی که بازارهای دیجیتال ژاپن با آن روبرو هستند، تسلط فزاینده شرکت‌های فناوری خارجی، به‌ویژه شرکت‌های آمریکایی و چینی است. این امر مشاغل داخلی را در مضیقه قرار داده و نگرانی‌هایی را در مورد حفظ حریم خصوصی و امنیت داده‌ها ایجاد کرده است. علاوه بر این، مقررات ژاپن در مورد جمع‌آوری و استفاده از داده‌ها، پراکنده و قدیمی هستند و برای کسب‌وکارها و مصرف‌کنندگان سردرگمی ایجاد می‌کنند. برای مقابله با این چالش‌ها، سیاست‌گذاران باید محیط عادلانه‌تری را برای کسب‌وکارهای داخلی ایجاد کنند و در عین حال مقررات را برای تضمین حفظ حریم خصوصی و امنیت داده‌ها بهبود بخشند.

چالش مهم دیگر برای بازارهای دیجیتال ژاپن، نیاز به مقررات کارآمدتر است. محیط نظارتی کنونی در ژاپن پیچیده و بوروکراتیک است و رقابت استارت‌آپ‌ها و کسب‌وکارهای کوچک با بازیگران بزرگ‌تر و با سابقه را دشوار می‌کند. علاوه بر این، مقررات ژاپن در مورد تجارت الکترونیک و سایر فعالیت‌های دیجیتال قدیمی است و واقعیت‌های عصر دیجیتال را منعکس نمی‌کند. برای مقابله با این چالش‌ها، سیاست‌گذاران باید مقررات را ساده کرده و محیط حمایتی بیشتری برای نوآوری و کارآفرینی در فضای دیجیتال ایجاد کنند. با انجام این اقدامات، ژاپن می‌تواند از رقابتی بودن بازارهای دیجیتال خود و رشد اقتصادی آن‌ها در سال‌های آتی اطمینان حاصل کند.



Japan's Precarious Digital Markets Crossroads

Shane Tews

AEI

January 13, 2023

عنوان

نویسنده

مرکز مطالعاتی

تاریخ انتشار

نقش دولت در ترویج نرم افزار منبع باز

نرم افزارهای منبع باز (OSS) در سراسر جهان توجه دولت‌ها را به خود جلب کرده است. در این خصوص مرکز مطالعات استراتژیک و بین‌المللی^۱ (CSIS) طی یک پروژه تحقیقاتی نشان می‌دهد که رویکرد هرکدام از کشورها در استفاده از نرم افزارهای منبع باز چگونه بوده است. برای تکمیل این پروژه از اطلاعات و داده‌های در دسترس عموم استفاده شده است. همچنین برای فهم سیاست موجود کشورهای گوناگون، محققان از ترجمه گزارش‌ها و یادداشت‌های غیررسمی موجود بهره بردند. این تحقیق بین ژانویه تا اوت ۲۰۲۲ انجام شد. با این حال محققان تنها به این تاریخ اکتفا نکرده و سیاست‌ها و لویایح مستند و مرتبط بعد از این تاریخ را نیز به پژوهش افزوده‌اند.

گزارش تفصیلی «نقش دولت در ترویج نرم افزار منبع باز» که توسط CSIS در ماه مه سال ۲۰۲۱ منتشر شد، اهمیت نرم افزار منبع باز و نقشی را که دولت‌ها می‌توانند در ارتقای توسعه و پذیرش آن ایفا کنند، مورد بحث قرار می‌دهد. نرم افزار منبع باز مزایای قابل توجهی از جمله صرفه‌جویی در هزینه، افزایش نوآوری و بهبود امنیت سایبری دارد. با این حال، نرم افزار متن باز علی‌رغم این مزایا، در بسیاری از سازمان‌های خصوصی و دولتی به دلیل عدم درک یا اعتماد به قابلیت‌های آن کم‌تر استفاده می‌شود.

این گزارش با تعریف نرم افزار متن باز به عنوان نوعی از نرم افزار آغاز می‌شود که در آن کد منبع برای مشاهده، تغییر و توزیع آزادانه برای همه در دسترس است. نویسندگان خاطرنشان می‌کنند با وجود اینکه نرم افزار اختصاصی می‌تواند گران‌تر و با ناسازگاری کمتر باشد، هنوز هم مدل نرم افزاری غالب و مورد استفاده بسیاری از دولت‌ها و سازمان‌ها است. با این حال، باکم شدن بودجه‌ها و تکامل فناوری، نرم افزار متن باز می‌تواند جایگزین مؤثری باشد که در هزینه‌ها صرفه‌جویی نموده و انعطاف‌پذیری بیشتری ارائه دهد.

یکی از مزایای اصلی نرم افزار منبع باز که توسط نویسندگان برجسته شده، توانایی آن در تقویت نوآوری است. از آنجاکه کد منبع به صورت رایگان در دسترس است، توسعه‌دهندگان از سراسر جهان می‌توانند به پایگاه کد کمک کرده و آن را قوی‌تر و سازگارتر کنند. علاوه بر این، از آنجایی که نرم افزار منبع باز اغلب به صورت مشترک توسعه می‌یابد، به احتمال زیاد برای رفع نیازهای خاص سفارشی می‌شود. این امر می‌تواند برای سازمان‌های دولتی که ممکن است الزامات خاصی برای نرم افزار خود داشته باشند، ارزشمند باشد.

یکی دیگر از مزایای نرم افزار منبع باز، پتانسیل آن برای بهبود امنیت سایبری است. از آنجایی که کد منبع برای هرکسی قابل بررسی است، شناسایی و رفع آسیب‌پذیری‌های امنیتی آسان‌تر است. این ویژگی برخلاف نرم افزار اختصاصی است که در آن آسیب‌پذیری‌ها ممکن است برای مدت زمان طولانی‌تری پنهان بمانند و به طور بالقوه سامانه‌ها را برای حمله باز بگذارند. با

۱. Open Source Software (OSS)

۲. Center for Strategic and International Studies (CSIS)

استفاده از نرم‌افزارهای منبع باز، دولت‌ها می‌توانند از امنیت سیستم‌های خود اطمینان بیشتری داشته باشند.

با وجود مزایای نرم‌افزار منبع باز، نویسندگان اشاره می‌کند که هنوز موانعی برای پذیرش آن وجود دارد. یکی از چالش‌های اصلی عدم درک یا اعتماد به قابلیت‌های نرم‌افزار منبع باز است. برخی از افراد ممکن است در استفاده از نرم‌افزاری که توسط فروشنده یا شرکت معروفی تولید نشده، شک داشته باشند. علاوه بر این، ممکن است نگرانی‌هایی در مورد پشتیبانی و نگهداری از نرم‌افزار منبع باز وجود داشته باشد، به خصوص اگر از این نرم‌افزار در سیستم‌های کلیدی استفاده شود.

به گفته نویسندگان، برای پرداختن به این چالش‌ها، دولت‌ها می‌توانند نقش مهمی در ترویج نرم‌افزار منبع باز ایفا کنند. یکی از این راه‌ها ارائه منابع و پشتیبانی برای توسعه نرم‌افزار منبع باز است. برای مثال اختصاص بودجه برای پروژه‌های نرم‌افزاری منبع باز و یا مشارکت با توسعه‌دهندگان نرم‌افزار از جمله راه‌های این پشتیبانی است.

راه دیگر ترویج نرم‌افزارهای منبع باز، ایجاد سیاست‌های تشویقی است. برای مثال، وضع دستورالعمل‌های توسعه سامانه‌های جدید با رویکرد منبع باز توسط دولت یک اقدام راهبردی است. همچنین اجبار به توسعه نرم‌افزارها در بخش‌های دولتی با رویکرد منبع باز از دیگر راهکارهای پیشنهادی است. با اجرای چنین سیاست‌هایی، دولت‌ها می‌توانند به پذیرش نرم‌افزار منبع باز کمک کنند.

در پایان، استفاده دولت‌ها از قدرت خرید خود برای ترویج نرم‌افزار منبع باز است. دولت‌ها می‌توانند با جستجوی فروشندگانی که از نرم‌افزار منبع باز استفاده می‌کنند، به ایجاد بازاری برای نرم‌افزارهای منبع باز کمک کنند. این کار فروشندگان را تشویق می‌کند تا پیشنهادهای منبع باز بیشتری را توسعه دهند که در درازمدت به نفع دولت‌ها و سایر سازمان‌ها خواهد



Government's Role in Promoting Open Source Software
 Georgia Wood and Eugenia Lostrì
 CSIS
 January 9, 2023

عنوان
 نویسنده
 مرکز مطالعاتی
 تاریخ انتشار

پایان

نگاهی نو،
به حکمرانی فضای مجازی



تهران، ضلع غربی میدان فلسطین، خیابان آیت الله طالقانی، پلاک ۳۹۷
۰۲۱-۸۶۰۵۴۲۹۱

www.zaviehmag.ir

[@zaviehmag](#)

نشانی
تلفن
وبسایت
شبکه‌های اجتماعی