زاویه
نگاهی نو؛
به حکمرانی فضای مجازی

دوره اول
شماره ۹

رصدنامه حکمرانی سایبری

مروری بر اندیشکده‌های شاخص جهان | اسفند ۱۴۰۱

دوره ۱، شماره ۹، اسفند ۱۴۰۱

رصدنامه حکمرانی سایبری

مروری بر اندیشکده‌های شاخص جهان

تهیه‌وتنظیم و ناظر علمی: امیرعباس رکنی، امین زاده‌حسین

نشانی: تهران، ضلع غربی میدان فلسطین، خیابان آیت‌الله طالقانی، پلاک ۳۹۷

تلفن و وبسایت: ۰۲۱-۸۶۰۵۴۲۹۱ www.sccm.ir

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

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. همچنین 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:

اهم اندیشکده‌های آمریکایی

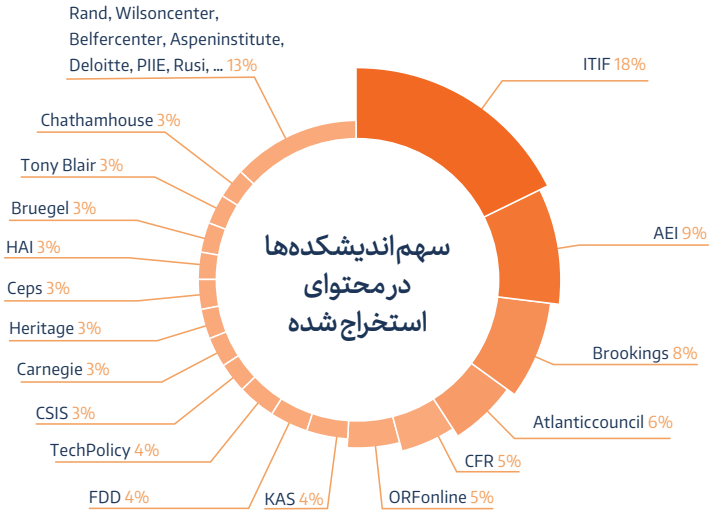
- امریکن اینترپرایز
- بروکینگز
- هریتیج
- شورای آتلانتیک
- بِلفِر
- رَند
- کارنگی
- پیو
- ویلسون
- شورای روابط خارجی
- مؤسسه اقتصاد بین‌الملل پیترسون
- مؤسسه هادسون
- مرکز مطالعات استراتژیک و بین‌المللی

اهم اندیشکده‌های غیرآمریکایی

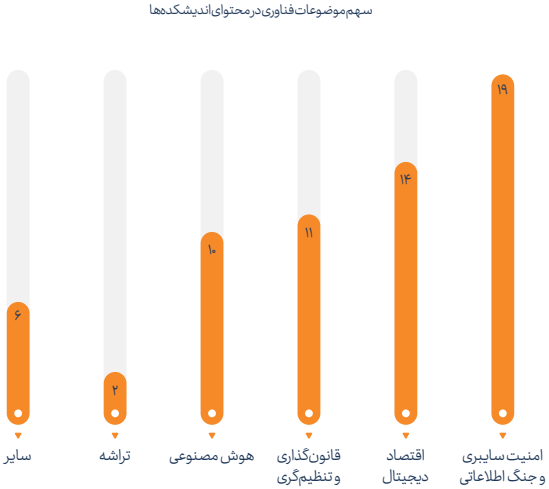
- چتم هاوس
- بروگل
- مؤسسه امور بین‌الملل و اروپا
- بنیاد فناوری اطلاعات و نوآوری
- مرکز مطالعات سیاست اروپا

در این شماره از رصد که در بازه یک‌ماهه اسفندماه نگارش شده است، ۱۲۰ عنوان استخراج شد که شامل گزارش، رویداد مجازی، یادداشت، پروژه‌های تحقیقاتی و... می‌شود.

باتوجه‌به نمودار زیر، بنیاد نوآوری و فناوری اطلاعات «ITIF» با ۱۸ بیشترین محتوای تولیدی مرتبط با فضای مجازی را به خود اختصاص داد و بعد از آن امریکن اینترپرایز «AEI» با ۹ درصد، بروکینگز «Brookings» با ۸ درصد، شورای آتلانتیک «Atlantic Council» با ۶ درصد، شورای روابط خارجی «CFR» و بنیاد آبزرور «ORFonline» هرکدام با ۵ درصد، بنیاد کنراد آدناور «KAS»، بنیاد دفاع از دموکراسی‌ها «FDD» و سیاست فناوری «Tech Policy» هرکدام با ۴ درصد، مرکز مطالعات استراتژیک و بین‌المللی «CSIS»، کارنگی «Carnegie»، هریتیج «Heritage»، مرکز مطالعات سیاستی اروپا «CEPS»، اندیشکده هوش مصنوعی دانشگاه استنفورد «HAI»، بروگل «Bruegel»، چتم‌هاوس «ChathamHouse» و مؤسسه تونی‌بلیر «Tony Blair» هرکدام با ۳ درصد و سایر اندیشکده‌ها، مشترکاً در تولید ۱۳ درصد از محتوا سهیم بوده‌اند..

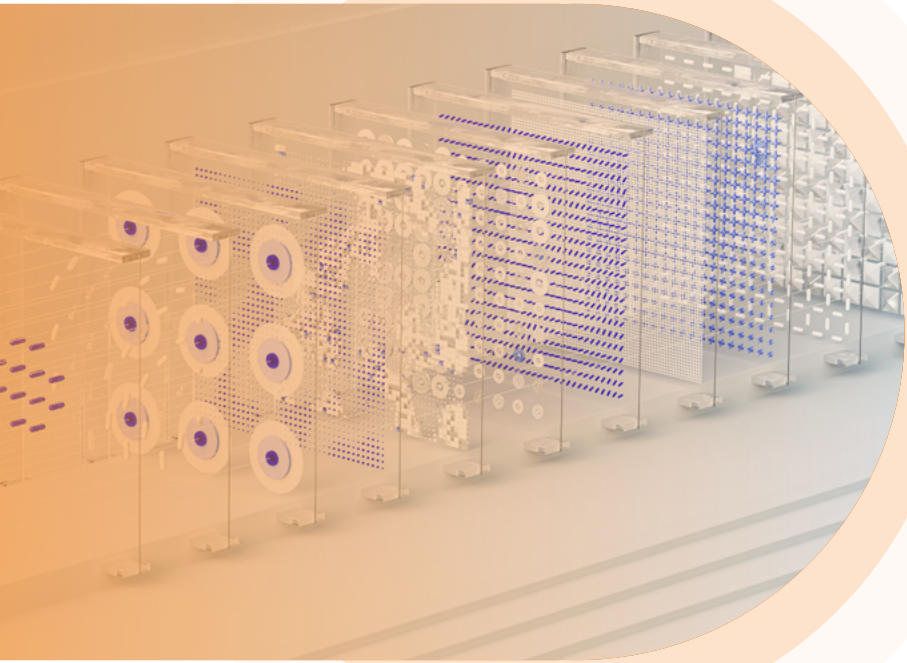


مطالب مستخرج طبق یک طبقه‌بندی موضوعی که از پیش تعیین شده بود در دسته‌های هوش مصنوعی، اقتصاد دیجیتال، امنیت سایبری و جنگ اطلاعاتی، قانون‌گذاری و تنظیم‌گری، تراشه و سایر تقسیم شدند که فراوانی مطالب هر دسته موضوعی به شرح زیر است:



۱۲۰ عنوان اندیشکده‌های شاخص جهان در اسفندماه، دربرگیرنده بیش از ۴۵۰ هزار کلمه محتوا می‌باشد که توسط ۲۴۳ اندیشمند تولید و نگارش شده‌اند. محتوای استخراج‌شده شامل گزارش‌ها، آمارها، یادداشت‌ها و مقالات علمی هستند.

در ادامه به بررسی ۶۲ عنوان برگزیده از ۱۲۰ گزارش استخراج شده پرداخته شده است.



گزارش‌های برگزیده

هوش مصنوعی

اختراعات هوش مصنوعی: گزینه‌های سیاستی و مسیر پیش رو

گزارش «اختراعات هوش مصنوعی: گزینه‌های سیاستی و مسیر پیش رو» از اندیشکده بروکینز، چالش‌های ناشی از اختراعات هوش مصنوعی، وضعیت فعلی سیستم ثبت اختراع و راه‌حل‌های بالقوه سیاستی را مورد بحث قرار می‌دهد. نویسنده با تشریح مسائل مختلف در خصوص اختراعات هوش مصنوعی بحث خود را آغاز می‌کند، ازجمله این واقعیت که ممکن است قوانین ثبت اختراع فعلی برای تنظیم این نوع فناوری نامناسب باشد. به استدلال او این امر می‌تواند منجر به عدم اطمینان و ناکارآمدی در سیستم ثبت اختراع شود و حتی ممکن است از نوآوری جلوگیری کند.

به همین منظور، راه‌حل‌های سیاستی بالقوه برای رسیدگی به این مسائل مورد بررسی قرار می‌گیرد. یکی از گزینه‌های موجود، **بازنگری قوانین ثبت اختراع برای توضیح بهتر اختراعات هوش مصنوعی است که می‌تواند شامل تغییراتی در تعریف «مخترع» یا معیارهای ثبت اختراع باشد.** گزینه دیگر ایجاد نوع جدیدی از حق مالکیت معنوی برای هوش مصنوعی به‌طور خاص است (نظام افتراقی مالکیت معنوی)، مانند «حق ثبت اختراع نوآوری در هوش مصنوعی». راه‌حل‌های سیاستی بالقوه دیگری، مانند ایجاد یک سامانه مرکزی برای ثبت اختراعات هوش مصنوعی یا اجرای الزامات افشای اجباری برای اختراعات تولیدشده توسط هوش مصنوعی نیز مطرح می‌شود. با این وجود، این گزینه‌ها می‌تواند صرفاً به رفع برخی از چالش‌های ناشی از اختراعات هوش مصنوعی کمک کند و ممکن است دارای اشکالات و پیامدهای ناخواسته‌ای نیز باشد.

به‌طورکلی، این گزارش بر نیاز سیاست‌گذاران به بررسی دقیق پیامدهای اختراعات هوش مصنوعی و توسعه سیاست‌هایی که نوآوری را ترویج و از منافع عمومی محافظت می‌کند، تأکید دارد. برای دستیابی به این هدف اتخاذ یک رویکرد مشارکتی، شامل ورودی‌های ذی‌نفعان در بخش‌های خصوصی و دولتی، ضروری است.

عنوان	AI inventions: Policy options and a path forward
نویسنده	John Villasenor
مرکز مطالعاتی	Brookings
تاریخ انتشار	March 6, 2023

دست‌یابی به تعریف هوش مصنوعی در پرتو قانون هوش مصنوعی اتحادیه اروپا

اتحادیه اروپا (EU) قانون هوش مصنوعی (AI) را معرفی کرده که در پی تنظیم توسعه و استفاده از هوش مصنوعی در اتحادیه اروپا است. تعریف هوش مصنوعی در این قانون از باب تعیین فعالیت‌های ذیل چارچوب نظارتی از اهمیت بالایی برخوردار است. این گزارش توسط مرکز مطالعات سیاست اروپا (CEPS) منتشرشده و توضیحاتی در مورد تعریف هوش مصنوعی آن‌طور که در قانون اتحادیه اروپا آمده، ارائه می‌دهد.

نکات کلیدی زیر در خصوص تعریف هوش مصنوعی در قانون اتحادیه اروپا قابل‌توجه است:

۱. تعریف گسترده از هوش مصنوعی: قانون، هوش مصنوعی را این‌گونه تعریف می‌کند: «نرم‌افزاری که با یک یا چند فن و رویکرد ذکرشده در پیوست ۱ توسعه‌یافته و می‌تواند برای مجموعه‌ای از اهداف معین که توسط انسان تعریف‌شده، خروجی‌هایی مانند محتوا، پیش‌بینی، توصیه‌ها یا تصمیم‌هایی را تولید کرده و انجام دهد که بر محیط‌هایی که با آن‌ها در تعامل است، تأثیر می‌گذارد.»؛ این تعریف عمداً گسترده شده است تا کاربردهای بسیاری از هوش مصنوعی را پوشش دهد.

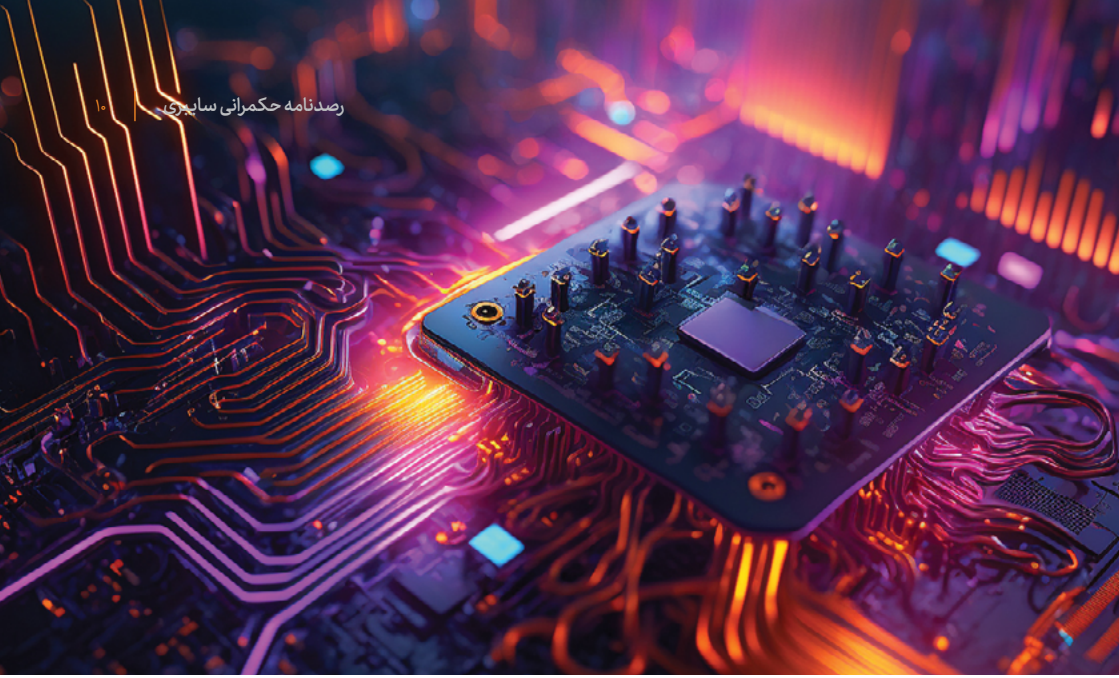
۲. نقش ضمیمه ۱: ضمیمه ۱ قانون هوش مصنوعی فنون و رویکردهایی را برمی‌شمارد که واجد شرایط هوش مصنوعی هستند. فن‌های ذکرشده در این ضمیمه شامل یادگیری ماشینی، یادگیری عمیق و سیستم‌های مبتنی‌بر قانون و ... است. این ضمیمه حصری نبوده و امکان گنجاندن فن‌های جدید با توسعه هوش مصنوعی را فراهم می‌کند.

۳. مستثنیات تعریف: تعریف هوش مصنوعی در قانون هوش مصنوعی، فناوری‌های خاصی مانند سیستم‌های خودکار غیر نرم‌افزاری، پردازش زبان طبیعی و رابط‌های کاربری را مستثنا می‌کند.

۴. خنثی بودن تعریف: تعریف هوش مصنوعی در قانون فوق، به لحاظ فناوری خنثی است؛ به این معنی که به هیچ فناوری یا برنامه خاصی وابسته نیست. این امر اجازه می‌دهد تا با تکامل هوش مصنوعی و ظهور فناوری‌های جدید، این تعریف موضوعیت خود را از دست ندهد.

۵. رویکرد ریسک‌محور: قانون هوش مصنوعی رویکردی مبتنی‌بر ریسک در مقررات با سطوح مختلف بسته به خطرات بالقوه مرتبط با برنامه‌های کاربردی هوش مصنوعی اتخاذ می‌کند. تعریف هوش مصنوعی یک عنصر کلیدی در تعیین میزان مقرراتی است که برای یک برنامه کاربردی هوش مصنوعی اعمال می‌شود.

۶. همسویی با استانداردهای بین‌المللی: تعریف هوش مصنوعی در این قانون با استانداردهای بین‌المللی، مانند استاندارد ISO/IEC 2382-1 در خصوص اصطلاحات هوش مصنوعی هم‌راستا است.



۷. شفافیت برای ذی‌نفعان: تعریف هوش مصنوعی در قانون فوق در مورد اینکه کدام فعالیت‌ها تحت چارچوب نظارتی قرار می‌گیرند، با ذی‌نفعان شفاف است. این شفافیت برای ارتقای نوآوری و سرمایه‌گذاری در هوش مصنوعی و حصول اطمینان از توسعه و استفاده مسئولانه و قابل‌اعتماد از این فناوری مهم است.

* *

عنوان	What's in a name?
نویسنده	Andrea Renda, Alex Engler
مرکز مطالعاتی	Ceps
تاریخ انتشار	February 22, 2023

قدرت اقناع سیاسی هوش مصنوعی

گزارش «قدرت اقناع سیاسی هوش مصنوعی» در مؤسسه هوش مصنوعی انسان‌محور (HAI) دانشگاه استنفورد منتشر شده و به بررسی تأثیر هوش مصنوعی بر اقناع سیاسی، تصمیم‌گیری‌های دموکراتیک و برنامه‌های کاربردی هوش مصنوعی در این حوزه، خطرات بالقوه و نیاز به مقررات و دستورالعمل‌های اخلاقی می‌پردازد. هوش مصنوعی پتانسیل افزایش مبارزات سیاسی را دارد و می‌تواند برای دست‌کاری افکار عمومی و تضعیف ارزش‌های دموکراتیک نیز مورد استفاده قرار گیرد. روش‌های استفاده از هوش مصنوعی در کمپین‌های سیاسی، شامل تبلیغات هدفمند، تحلیل احساسات و نظارت بر رسانه‌های اجتماعی می‌شود. این فن‌ها به احزاب و نامزدهای سیاسی کمک می‌کند تا اقدام به جمعیت‌شناسی کرده و پیام‌های خود را طوری تنظیم کنند که برای مخاطبان جذاب باشد؛ اما قابلیت استفاده از این روش‌ها برای اهداف پلید، مانند انتشار اخبار جعلی، دست‌کاری احساسات و سرکوب مخالفان نیز وجود دارد.

نگرانی‌های اخلاقی درخصوص استفاده از هوش مصنوعی در مبارزات سیاسی، همچون پتانسیل تعصب الگوریتمی، عدم شفافیت و خطر افزایش قطبی‌سازی و تکه‌تکه شدن جامعه نیز قابل توجه هستند. در شرایط کنونی، فقدان مقررات و دستورالعمل‌های اخلاقی در این خصوص، زمینه سوءاستفاده و دست‌کاری افکار عمومی را میسر و یکپارچگی فرایندهای دموکراتیک را تضعیف می‌کند. برای رفع این نگرانی‌ها، نویسنده برخی دستورالعمل‌های اخلاقی را برای استفاده از هوش مصنوعی در اقناع سیاسی پیشنهاد می‌کند، مانند دستورالعمل‌های شفافیت، انصاف، مسئولیت‌پذیری و حفاظت از حریم خصوصی و آزادی بیان.

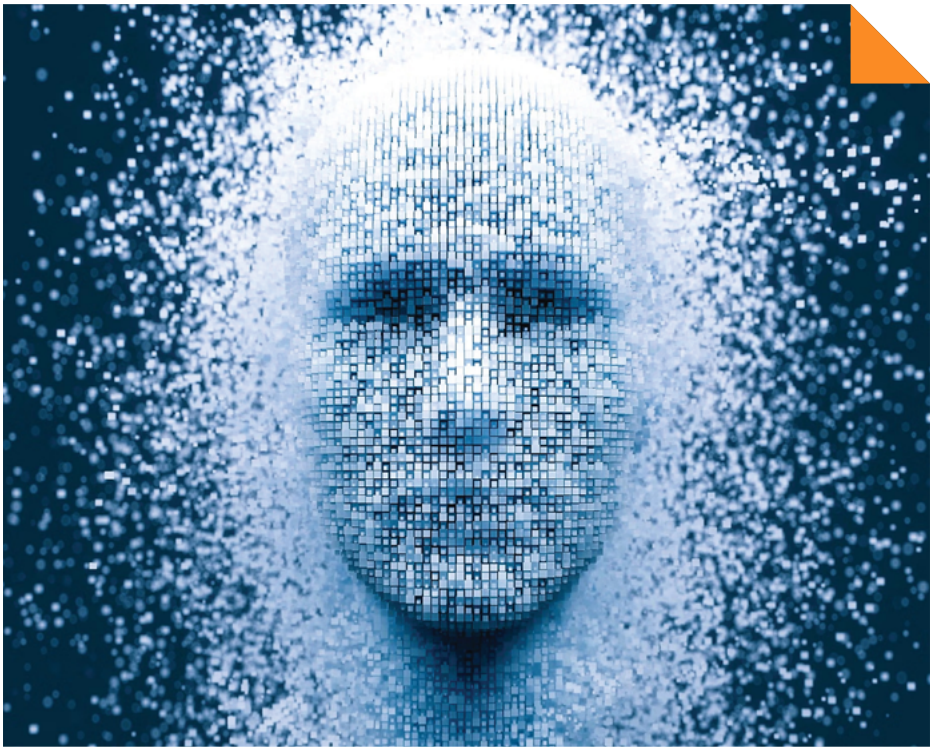
این گزارش به بررسی نقش هوش مصنوعی در کمپین‌های اخبار جعلی با استفاده از قابلیت دیپ‌فیک‌های تولیدشده توسط هوش مصنوعی برای دست‌کاری افکار عمومی نیز می‌پردازد. تشخیص مدیاهای تولیدشده توسط هوش مصنوعی از محتوای معتبر دشوار است و می‌توان از این موارد برای انتشار اخبار جعلی، تضعیف اعتماد به نهادهای دموکراتیک و افزایش قطبی‌سازی استفاده کرد. جهت کاهش این خطرات، برخی راه‌حل‌های فنی، مثل توسعه الگوریتم‌هایی برای شناسایی دیپ‌فیک‌ها و ارتقای سواد رسانه‌ای برای کمک به عموم مردم برای تمایز بین محتوای واقعی و جعلی باید مورد توجه قرار بگیرد. **به این منظور، همکاری بین دولت‌ها، شرکت‌های فناوری و سازمان‌های جامعه مدنی برای پیگیری اقدامات متقابل مؤثر در برابر کمپین‌های اخبار جعلی ضروری است.** با تحقق این همکاری از توسعه و استقرار هوش مصنوعی به‌گونه‌ای که ارزش‌های دموکراتیک را حفظ نموده و از شهروندان در برابر دست‌کاری و سوءاستفاده محافظت کند، اطمینان حاصل خواهد شد. به نظر می‌رسد، ایجاد یک جنبش «**هوش مصنوعی دموکراتیک**» که توسعه و استفاده از هوش مصنوعی را به روش‌هایی با اولویت نهادن به ارزش‌های انسانی و اصول دموکراتیک هدایت می‌کند، کمک‌کننده است.

عنوان	AI's Powers of Political Persuasion
نویسنده	Andrew Myers
مرکز مطالعاتی	HAI
تاریخ انتشار	February 27, 2023

عصر هوش مصنوعی در مقابل عصر پوپولیسم

جیمز پتوکوکیس[۱] تحلیل‌گر برجسته سیاسی و کارشناس فناوری در گزارش اخیر خود به نام «عصر هوش مصنوعی در مقابل عصر پوپولیسم» در مؤسسه امریکن اینترپرایز (AEI) تضاد احتمالی بین این دو پدیده مهم را بررسی کرده و مسیری را برای کاهش این تضاد پیشنهاد می‌کند. او معتقد است با اینکه هوش مصنوعی پتانسیل مزایای قابل‌توجهی را دارد، خطر تشدید شکاف‌های سیاسی و اجتماعی که به جنبش‌های پوپولیستی در سراسر جهان دامن می‌زند را نیز در پی خواهد داشت.

این گزارش با تعریف پوپولیسم و تشریح ویژگی‌های کلیدی آن شروع می‌کند. پوپولیسم یک ایدئولوژی سیاسی نیست، بلکه مجموعه‌ای از تاکتیک‌هایی است برای کسب قدرت از طریق حمایت مردمی علیه نخبگان. پوپولیسم‌ها معمولاً مسائل را در قالب «مردم» در مقابل «سازمان» می‌نگرند و از لفاظی‌های ضد نخبه‌گرایی استفاده می‌کنند. پوپولیسم مختص هیچ کشور یا منطقه‌ای نیست، بلکه پدیده‌ای جهانی است که در سال‌های اخیر افزایش یافته است.



۱. James Pethokoukis

در سال‌های اخیر و به لطف فناوری‌های نوظهور همانند هوش مصنوعی، روش‌های مختلفی با پتانسیل تشدید پوپولیسم به وجود آمده است. فرایند بهره‌برداری پوپولیست‌ها از هوش مصنوعی از سه مرحله کلیدی تشکیل می‌شود:

۱. هوش مصنوعی می‌تواند با خودکار کردن مشاغل و افزایش تمرکز ثروت در دست عده‌ای خاص به نابرابری اقتصادی بیشتر بیانجامد.
۲. هوش مصنوعی می‌تواند با تکیه بر داده‌هایی که تبعیض‌های گذشته را تکرار می‌کند، تعصبات و سوگیری‌های کنونی را تقویت کند.
۳. هوش مصنوعی می‌تواند قدرت و فرصت دست‌کاری افکار عمومی را در اختیار رهبران پوپولیست قرار دهد و با اجازه دادن به آن‌ها جهت تنظیم پیام‌های خود برای گروه‌های خاصی از رأی‌دهندگان که همان محرومان و تبعیض‌دیده‌گان هستند، این کار را آسان‌تر کند.

برای کاهش این خطرات، سیاست‌گذاران باید اقدامات زیر را با فوریت انجام دهند:

- سیاست‌گذاران باید در رسیدگی به اختلالات اقتصادی نشأت گرفته از هوش مصنوعی فعال باشند. سرمایه‌گذاری در برنامه‌های آموزشی جهت کمک به کارگران برای انتقال به صنایع جدید و ارائه شبکه‌های ایمنی اجتماعی برای حمایت از بازماندگان ازجمله کارهایی است که سیاست‌گذاران می‌توانند انجام دهند.
- سیاست‌گذاران باید اقداماتی را انجام دهند تا از توسعه و استقرار هوش مصنوعی به شیوه‌ای اخلاقی و مسئولانه اطمینان حاصل شود. ارتقای تنوع در صنعت فناوری و ایجاد چارچوب‌های نظارتی جهت اطمینان از عدم استفاده از هوش مصنوعی برای تبعیض علیه گروه‌های اقلیتی، ازجمله کارهایی است که سیاست‌گذاران می‌توانند انجام دهند.
- سیاست‌گذاران باید در مقابل سوءاستفاده احتمالی از هوش مصنوعی توسط رهبران پوپولیست احتیاط کنند. ارتقای سواد رسانه‌ای و تأمین بودجه برای روزنامه‌نگاری مستقل جهت مقابله با اطلاعات نادرست و تبلیغات ازجمله کارهایی است که سیاست‌گذاران می‌توانند انجام دهند.

در پایان باید توجه داشت که علی‌رغم آن‌که هوش مصنوعی پتانسیل تشدید و افزایش پوپولیسم را دارد، پتانسیل کمک به رفع آن را نیز دارد. هوش مصنوعی می‌تواند برای برابری اقتصادی بیشتر، کاهش تعصب و تبعیض و تقویت اشکال فراگیر دموکراسی مورد استفاده قرار گیرد؛ اما تحقق این موارد مستلزم آن است که سیاست‌گذاران اقدام به شکل دادن به توسعه و استقرار هوش مصنوعی به شیوه‌هایی هماهنگ با ارزش‌های دموکراتیک و مطابق با منافع عمومی نمایند.

عنوان	The Age of AI vs. the Age of Populism
نویسنده	James Pethokoukis
مرکز مطالعاتی	AEI
تاریخ انتشار	March 08, 2023

هوش مصنوعی آموزش و یادگیری را متحول خواهد کرد!

گزارش «هوش مصنوعی آموزش و یادگیری را متحول خواهد کرد» در مؤسسه هوش مصنوعی انسان‌محور استنفورد (HAI) منتشر شده و در مورد نقش هوش مصنوعی در آموزش و نیاز به اطمینان از اجرای هوش مصنوعی به نفع دانش‌آموزان و معلمان بحث می‌کند.

هوش مصنوعی قابلیت تغییر شیوه آموزش را دارد، اما ریسک و چالش‌هایی را نیز به همراه دارد که باید مورد توجه قرار گیرد. مزایای بالقوه هوش مصنوعی در آموزش شامل یادگیری شخصی، ارزیابی و بازخورد بهبودیافته و افزایش دسترسی در دانش‌آموزان معلول می‌شود. در مقابل، خطرات هوش مصنوعی نیز شامل تعصب الگوریتمی، مسائل مربوط به حریم خصوصی و پتانسیل بالای آن برای جایگزینی معلمان انسانی است.

بر همین اساس، حصول اطمینان از توسعه و پیاده‌سازی هوش مصنوعی به‌صورت شفاف، اخلاقی و مسئولانه اهمیت بالای دارد. منظور از شفافیت، قابل توضیح بودن و پاسخگو بودن سیستم‌های هوش مصنوعی است و مشارکت معلمان و دانش‌آموزان در طراحی و پیاده‌سازی سیستم‌های هوش مصنوعی در آموزش، اهمیت بالایی در مبحث شفافیت پیدا می‌کند.

برخی از اصول استفاده مسئولانه از هوش مصنوعی در آموزش عبارت است از: حصول اطمینان از توسعه و استفاده از سیستم‌های هوش مصنوعی به نفع دانش‌آموزان، شفافیت و قابل توضیح بودن این سیستم‌ها، عدم تقویت یا تشدید نابرابری‌ها و توسعه و پیاده‌سازی همگام با نظرات معلمان و دانش‌آموزان.

این گزارش توصیه‌هایی را هم برای سیاست‌گذاران و رهبران آموزشی در خصوص اطمینان از اجرای مسئولانه و مؤثر هوش مصنوعی عنوان می‌کند. این توصیه‌ها شامل سرمایه‌گذاری در تحقیق در مورد تأثیر هوش مصنوعی در آموزش، ارائه راهنمایی و پشتیبانی به معلمان و مدارس در مورد نحوه استفاده مؤثر از هوش مصنوعی و اطمینان از تحت نظارت بودن سیستم‌های هوش مصنوعی است.

از دیگر محورهای این گزارش حصول اطمینان از استفاده از هوش مصنوعی برای تقویت و حمایت از معلمان انسانی به‌جای جایگزینی آن‌ها است؛ بدین معنی که هوش مصنوعی باید برای تقویت قابلیت‌های انسانی، مانند ارائه بازخوردهای شخصی و شناسایی حوزه‌هایی که دانش‌آموزان در آن نیازمند حمایت بیشتری هستند، استفاده شود. سیستم‌های هوش مصنوعی باید به‌گونه‌ای طراحی و پیاده‌سازی شود که برای همه دانش‌آموزان جامع و قابل‌دسترس بوده و نباید تعصبات نژادی، جنسیتی و ... را تقویت کرده یا تداوم بخشد.

عنوان	.AI Will Transform Teaching and Learning. Let's Get it Right
نویسنده	Claire Chen
مرکز مطالعاتی	HAI
تاریخ انتشار	March 9, 2023

به چین اجازه ندهید آینده هوش مصنوعی را تعیین کند

گزارش مؤسسه هادسون تحت عنوان «به چین اجازه ندهید آینده هوش مصنوعی را تعیین کند» به بررسی چالش‌های برخاسته از استراتژی چین برای سرمایه‌گذاری هنگفت در هوش مصنوعی جهت نیل به برتری فناورانه نسبت به ایالات‌متحده و سایر کشورها پرداخته و استدلال می‌کند ایالات‌متحده و متحدانش برای حفظ رهبری خود در تحقیق و توسعه هوش مصنوعی می‌بایست اقدامات پیشگیرانه‌ای انجام دهند و از تسلط چین بر این حوزه جلوگیری کنند.

این گزارش ابتدا وضعیت فعلی تحقیق و توسعه هوش مصنوعی در چین و سرمایه‌گذاری گسترده این کشور در این زمینه و اهداف بلندپروازانه دولت چین در حوزه توسعه هوش مصنوعی را بررسی کرده و نتیجه می‌گیرد که تمرکز چین بر هوش مصنوعی نه‌تنها به خاطر منافع اقتصادی، بلکه با اهداف استراتژیک گسترده‌تری همچون اهداف نظامی و ژئوپلیتیکی هدایت می‌شود.

بر همین اساس، اگر ایالات‌متحده و متحدانش امیدوارند رهبری خود در این موضوع را حفظ کنند، باید در زمینه تحقیق و توسعه هوش مصنوعی فعال‌تر بوده و با انجام اقدامات حیاتی، مانند افزایش سرمایه‌گذاری در تحقیق و توسعه هوش مصنوعی، تمرکز بیشتر بر ملاحظات اخلاقی در توسعه هوش مصنوعی و همکاری قوی‌تر بین دولت‌ها، دانشگاه‌ها و بخش خصوصی از جایگاه خود و ملت‌هایشان دفاع کنند. در این خصوص، درک اهمیت همکاری بین‌المللی در توسعه هوش مصنوعی یک ضرورت استراتژیک است. ایالات‌متحده و متحدانش باید برای ایجاد استانداردها و هنجارهای مشترک جهت توسعه و استقرار فناوری‌های هوش مصنوعی با یکدیگر همکاری کنند و برای ایجاد و توسعه اصول اخلاقی در استفاده از هوش مصنوعی، تلاش‌های بین‌المللی را راهبری کرده و چارچوبی مشترک برای تنظیم فناوری‌های هوش مصنوعی ایجاد کنند.

از سوی دیگر، ایالات‌متحده باید برای محدود کردن دسترسی چین به تحقیق و توسعه در حوزه هوش مصنوعی اقدامات ویژه‌ای را در پیش بگیرد، اقداماتی همچون محدودیت در صادرات فناوری‌های حساس و افزایش نظارت بر سرمایه‌گذاری‌های چین در شرکت‌های آمریکایی که روی هوش مصنوعی کار می‌کنند.

عنوان	Don't Let China Determine the Future of Artificial Intelligence
نویسنده	Arthur Herman
مرکز مطالعاتی	Hudson
تاریخ انتشار	March 13, 2023

هوش مصنوعی چگونه می‌تواند برای ما قانون بنویسد؟

گزارش «هوش مصنوعی چگونه می‌تواند برای ما قانون بنویسد» در مرکز علوم و امور بین‌الملل بلفر در دانشگاه هاروارد منتشرشده و پتانسیل هوش مصنوعی برای ایفای نقش در سیستم حقوقی، به‌ویژه در ایجاد قوانین را بررسی می‌کند. به استدلال این گزارش با اینکه هوش مصنوعی در حال حاضر در حرفه حقوق برای کمک به وظایفی مانند تحلیل اسناد و تحقیقات حقوقی استفاده می‌شود، پتانسیل آن بسیار فراتر از این است. برخی مزایای کلیدی استفاده از هوش مصنوعی در ایجاد قوانین به شرح ذیل هستند:

- هوش مصنوعی می‌تواند حجم وسیعی از داده‌ها را تجزیه‌وتحلیل نماید و الگوها و دیدگاه‌هایی را که انسان از آن‌ها مغفول مانده را شناسایی کند. این مهم می‌تواند به شناسایی شکاف‌های قوانین موجود یا حوزه‌هایی که قوانین جدید می‌طلبد کمک کند.
- هوش مصنوعی می‌تواند قوانین جدید را به‌سرعت و به طرز کارآمدی ایجاد کند که در مقایسه با فرایندهای قانونی سنتی در زمان و منابع صرفه‌جویی می‌کند.
- هوش مصنوعی می‌تواند با تحلیل عینی داده‌ها سوگیری‌های شناختی متداول را از فرایند قانون‌گذاری حذف کند.

در مقابل، برای استفاده از هوش مصنوعی در ایجاد قوانین برخی چالش‌ها و مخاطرات ذیل نیز باید مورد توجه قرار گیرند:

دشواری حصول اطمینان از منصفانه و عادلانه بودن قوانین نوشته شده به دست هوش مصنوعی؛ این امر نیازمند بررسی دقیق داده‌های مورد استفاده در آموزش الگوریتم‌های هوش مصنوعی و نظارت مداوم جهت اطمینان از شناسایی و رفع هرگونه سوگیری است. چالش دیگر تضمین شفافیت و پاسخگویی در روند قانون‌گذاری است. مهم است که شهروندان درک کنند، قوانین چگونه ایجاد می‌شوند و فرصتی برای ارائه نظرات خود داشته باشند.

برای رسیدگی به این چالش‌ها و استفاده از مزایای بالقوه هوش مصنوعی در ایجاد قوانین، دستورالعمل‌هایی جهت استفاده از هوش مصنوعی در فرایند قانون‌گذاری باید تدوین شود شود. این دستورالعمل‌ها باید حاوی اصولی چون شفافیت، انصاف و پاسخگویی باشد و دستوراتی در مورد داده‌هایی که می‌توان در آموزش الگوریتم‌های هوش مصنوعی از آن‌ها استفاده کرد و چگونگی اطمینان از شناسایی هرگونه سوگیری را در خود داشته باشند.

علاوه بر این، یک چارچوب نظارتی برای استفاده از هوش مصنوعی در فرایند قانون‌گذاری باید ایجاد شود. چنین چارچوبی باید دارای مکانیسم‌های نظارتی باشد تا از سازگاری قوانین ایجادشده توسط هوش مصنوعی با اصول قانونی و قانون اساسی اطمینان حاصل شود.

سرمایه‌گذاری در تحقیق و توسعه جهت بهبود قابلیت‌های هوش مصنوعی در فرایند قانون‌گذاری نیز باید مورد توجه قرار بگیرد. بهبود دقت و انصاف الگوریتم‌های هوش مصنوعی و توسعه رویکردهای جدید در تجزیه‌وتحلیل قانونی و تصمیم‌گیری ازجمله این موارد است.

در پایان نویسندگان به بررسی چندین نمونه از نحوه استفاده هوش مصنوعی در سیستم حقوقی پرداخته‌اند. مثلاً، در استونی، از یک الگوریتم هوش مصنوعی به نام «کرات»[۱] جهت شناسایی شکاف‌ها در قوانین موجود و پیشنهاد قوانین جدید استفاده می‌شود. در ایالات‌متحده، چندین ایالت چت‌بات‌های مبتنی‌بر هوش مصنوعی را برای کمک به شهروندان خود پیاده‌سازی کرده‌اند تا در مسیر رویه‌های قانونی و درک حقوق قانونی به شهروندان کمک کنند. این موارد پتانسیل هوش مصنوعی برای ایفای نقش مهم این فناوری در فرایند قانون‌گذاری را نشان می‌دهد.

۱. Kratt

عنوان	How AI Could Write Our Laws
نویسنده	Nathan Sanders, Bruce Schneier
مرکز مطالعاتی	Belfercenter
تاریخ انتشار	March 14, 2023

مقایسه GoogleBARD و ChatGPT

اندیشکده بروکینگز در یک گزارش جدید اقدام به مقایسه دو چت بات معروف Google BARD و ChatGPT کرده و سوگیری سیاسی، دقت واقعی و استدلال اخلاقی این دو مدل زبان قدرتمند هوش مصنوعی را با هم‌دیگر مقایسه می‌کند. BARD یک مدل زبانی است که گوگل آن را توسعه داده و برای تولید مقالات خبری و سایر اشکال محتوا استفاده می‌شود. ChatGPT نیز یک مدل زبان هوش مصنوعی است که توسط OpenAI توسعه یافته و برای تولید محتوا در طیف وسیعی از دامنه‌ها استفاده می‌شود. یافته‌ها حاکی از آن است که این مدل‌ها به‌شدت برای تولید مقالات خبری، پست‌های رسانه‌های اجتماعی و سایر اشکال محتوایی مناسب هستند و اگرچه پتانسیل سودمندی بالایی دارند، اما درعین‌حال پتانسیل‌های منفی آن‌ها در تولید و ترویج اخبار جعلی، تقویت تعصبات و دیدگاه‌های مضر باید مورد توجه قرار بگیرد.

به لحاظ سوگیری سیاسی، هر دو مدل شواهدی از سوگیری را نشان می‌دهند، BARD یک سوگیری محافظه‌کارانه خفیف و ChatGPT یک سوگیری لیبرال خفیف دارد. بااین‌حال، سوگیری‌های شناسایی‌شده نسبتاً کوچک بودند و تأثیر قابل‌توجهی بر خروجی کلی مدل‌ها نداشتند. به لحاظ **دقت واقعی**، هر دو مدل جز چند استثنا، عمدتاً دقیق هستند و هر دو مدل قادر به پاسخ دقیق به سؤالات مربوط به حقایق اساسی بودند، اما در خصوص پاسخ به سؤالات پیچیده‌تر یا سؤالاتی که نیاز به پاسخ‌های ظریف‌تری داشتند، دچار چالش می‌شدند. **از نظر استدلال اخلاقی**، هر دو مدل درجاتی از استدلال اخلاقی را نشان می‌دهند، اما کیفیت استدلال اخلاقی آن‌ها متفاوت است. هر دو مدل قادر به شناسایی معضلات اخلاقی و قضاوت اخلاقی بودند، اما قضاوت‌های انجام‌شده در این مدل‌ها اغلب بر اساس استدلال ساده یا ناقص بوده است.

این گزارش در نهایت در مورد پیامدهای این یافته‌ها در استفاده از مدل‌های زبان هوش مصنوعی در جامعه بحث می‌کند. با اینکه هر دو مدل BARD و ChatGPT دستاوردهای چشمگیری در هوش مصنوعی هستند، باز هم سؤالات مهمی در مورد تعصبات و محدودیت‌های بالقوه این مدل‌ها مطرح است. توسعه‌دهندگان مدل‌های زبان هوش مصنوعی برای رسیدگی به این مسائل باید اقدامات مسئولانه و بیشتری انجام دهند، اقداماتی مانند بهبود دقت و کیفیت مدل‌ها و اطمینان از شفافیت آن‌ها در مورد تعصبات و محدودیت‌های الگوریتمی.

عنوان	Comparing Google Bard with OpenAI's ChatGPT on political bias, facts, and morality
نویسنده	Darrell M. West
مرکز مطالعاتی	Brookings
تاریخ انتشار	March 23, 2023

به‌روزرسانی قانون و سیاست هوش مصنوعی: آیا بخش ۲۳۰ هوش مصنوعی مولد را پوشش می‌دهد؟

گزارش «به‌روزرسانی قانون و سیاست هوش مصنوعی: آیا بخش ۲۳۰ هوش مصنوعی مولد را پوشش می‌دهد؟» در مؤسسه هوش مصنوعی انسان‌محور (HAI) دانشگاه استنفورد منتشر شده و به بررسی پیامدهای قانونی استفاده از هوش مصنوعی مولد در تولید محتوا و پلتفرم‌های اشتراک‌گذاری تحت بخش ۲۳۰ قانون شایستگی ارتباطات[۱] (CDA) می‌پردازد. این گزارش چالش‌ها و فرصت‌هایی را که صنعت هوش مصنوعی با آن مواجه است، با تمرکز بر پیشرفت‌های GPT-۴، استفاده روزافزون از هوش مصنوعی در تصمیم‌گیری‌های قانونی، و استقرار هوش مصنوعی در برنامه‌های کاربردی مرتبط با قوانین در دنیای واقعی را برجسته می‌کند.

در ماه‌های اخیر، استقرار هوش و به خدمت گرفتن مصنوعی در تصمیم‌گیری‌های قانونی مورد توجه قرار گرفته است، بااین‌حال چالش‌ها و مخاطراتی که در ارتباط با استقرار هوش مصنوعی در این فرایندهای مهم وجود دارد باید مورد توجه قرار بگیرد. در ایالات‌متحده، بحث بر سر این است که آیا هوش مصنوعی مولد، مانند GPT-۴، تحت سپر مسئولیت بخش ۲۳۰ قرار می‌گیرد یا خیر؟ چنانچه هوش مصنوعی مشمول مصونیت قانونی قرار نگیرند، شرکت‌هایی که به این مدل‌ها تکیه می‌کنند، می‌توانند در قبال محتوای تولید شده توسط مسئول شناخته شوند که این امر منجر به افزایش دعوی قضایی احتمالی می‌شود. کمیسیون تجارت فدرال (FTC) به شرکت‌های هوش مصنوعی هشدار داده است که در مورد ادعاهای خود محتاط باشند و از صحت و اثبات آن‌ها اطمینان حاصل کنند. این امر نشان‌دهنده بررسی فزاینده برنامه‌های هوش مصنوعی توسط تنظیم‌گران در آمریکا است.

چالش‌های مربوط به حقوق مالکیت معنوی آثار تولیدشده توسط هوش مصنوعی نیز از دیگر ابعاد حقوقی موردتوجه تنظیم‌گران است که تاکنون نیز منجر به طرح برخی دعاوی و ایجاد چالش برای نظام قضایی آمریکا شده است. در تازه‌ترین اقدام، اداره کپی‌رایت ایالات‌متحده اعلام کرده است که برخی از آثار تولیدشده توسط هوش مصنوعی بسته به اینکه آیا اثر تولیدشده «نتیجه بازتولید مکانیکی» بوده یا «تصور ذهنی خود» نویسنده را منعکس می‌کند، ممکن است دارای حق نسخه‌برداری باشند.

۱. Communications Decency Act (CDA)

عنوان	?Law, Policy, & AI Update: Does Section 230 Cover Generative AI
نویسنده	Peter Henderson
مرکز مطالعاتی	HAI
تاریخ انتشار	March 23, 2023

هوش مصنوعی می‌تواند دولت‌ها را دموکراتیک کند

گزارش «هوش مصنوعی می‌تواند دولت‌ها را دموکراتیک کند» در اندیشکده سیاست فناوری منتشر شده و اذعان می‌کند فناوری هوش مصنوعی می‌تواند نقشی تحول‌آفرین در نحوه عملکرد دولت ایفا نموده و منجر به تصمیم‌گیری کارآمدتر و شفاف‌تر شده و نهایتاً ارزش‌های دموکراتیک را ارتقا دهد. حوزه‌هایی که هوش مصنوعی می‌تواند تأثیر بسیاری در آن داشته باشد، عبارت هستند از بهبود دسترسی به خدمات عمومی، افزایش ایمنی عمومی و مشارکت بیشتر شهروندان در دولت.

هوش مصنوعی با توانمند ساختن سازمان‌های دولتی در پردازش سریع و دقیق حجم زیادی از داده‌ها، می‌تواند کیفیت و کارایی خدمات عمومی را بهبود بخشد. این امر می‌تواند به خدمات شخصی‌تر برای شهروندان، تخصیص بهتر منابع و تصمیم‌گیری‌های سیاستی تأثیرگذارتر بیانجامد. مثلاً هوش مصنوعی می‌تواند در الگویابی داده‌های بهداشتی جهت درمان‌های شخصی‌تر بیماران یا در بهینه‌سازی جریان ترافیک برای کاهش ازدحام شهرها استفاده شود.

حوزه دیگری که هوش مصنوعی می‌تواند در آن تأثیر زیادی داشته باشد، حوزه امنیت عمومی است. ابزارهای مبتنی‌بر هوش مصنوعی می‌توانند در پیش‌بینی و پیشگیری از جرم و واکنش سریع‌تر و مؤثرتر به شرایط بحرانی به سازمان‌های مجری قانون کمک کنند. این امر می‌تواند جوامع را ایمن‌تر کرده و اعتماد عمومی بیشتری نسبت به نهادهای دولتی ایجاد کند.

هوش مصنوعی همچنین پتانسیل بالایی در افزایش مشارکت بیشتر شهروندان در دولت دارد. هوش مصنوعی با خودکار کردن برخی امور و کاهش بار کارکنان دولت، می‌تواند برای تعامل با شهروندان و جلب رضایت آن‌ها در تصمیم‌گیری‌های سیاستی فرصت‌های بیشتری فراهم کند. علاوه بر این، هوش مصنوعی می‌تواند حوزه‌هایی را که خدمات دولتی در آن‌ها ضعیف است، شناسایی کرده و شهروندان را قادر سازد تا بازخورد و پیشنهادهایی برای بهبود ارائه کنند.

باوجوداینکه هوش مصنوعی قابلیت ارتقای ارزش‌های دموکراتیک و بهبود عملکرد دولت را دارد، خطرات و چالش‌های بالقوه‌ای هم وجود دارد که باید به آن‌ها توجه کرد. مثلاً اگر الگوریتم‌های هوش مصنوعی تهیه شده برای داده‌های آموزشی نابرابری‌های موجود یا تبعیض را نمایان کنند، خطر سوگیری وجود دارد. همچنین نیاز به اطمینان از شفافیت و پاسخگویی در استفاده از هوش مصنوعی در سازمان‌های دولتی، مخصوصاً در حوزه‌هایی مانند اجرای قانون که در آن خطر سوءاستفاده وجود دارد، احساس می‌شود.

عنوان	Artificial Intelligence Could Democratize Government
نویسنده	Luke Hogg
مرکز مطالعاتی	Techpolicy
تاریخ انتشار	MArch 8, 2023

اقتصاد دیجیتال

رهایی ارزش از دگردیسی دیجیتال

گزارش جدید مؤسسه دیلویت به بررسی ارزش و بازده سرمایه‌گذاری[۱] (ROI)بر تحولات دیجیتال برای سازمان‌ها می‌پردازد. تحولات دیجیتال به سازمان‌ها کمک می‌کند تا عملیات خود را بهبود دهند، نوآوری کنند، مدل‌های تجاری جدید ایجاد کنند و تجربه مشتریان را بهبود دهند؛ اما بسیاری از سازمان‌ها به تعیین ارزش تحولات دیجیتال و بازگشت سرمایه مورد انتظار نمی‌پردازند.

یافته‌های این گزارش حاکی از آن است که سازمان‌هایی که تحولات دیجیتال را در اولویت قرار می‌دهند، با رشد درآمد و سودآوری بالاتر، نسبت به همتایان خود بهتر عمل می‌کنند. همچنین، سازمان‌هایی که به‌طور مؤثر بازده سرمایه گذاری ابتکارات دیجیتال خود را اندازه‌گیری می‌کنند، برای تصمیم‌گیری‌های مبتنی‌بر داده و تنظیم رویکرد خود موفق‌تر هستند.

از سوی دیگر، چالش‌های گوناگونی در خصوص اندازه‌گیری بازده سرمایه‌گذاری طرح‌های تحول دیجیتال وجود دارد. یکی از این چالش‌ها پیچیدگی تحولات دیجیتال است که ممکن است ذی‌نفعان، فناوری‌ها و فرایندهای متعددی را در بر گیرد. مضافاً، نسبت دادن نتایج خاص به تحولات دیجیتال می‌تواند دشوار باشد، زیرا عوامل بسیاری ممکن است در نتایج کسب‌وکار اثر داشته باشند.

برای غلبه بر این چالش‌ها، سازمان‌ها باید رویکردی جامع برای اندازه‌گیری بازده سرمایه‌گذاری در تحولات دیجیتال پیش بگیرند و تنها بر معیارهای مالی اتکا نکنند، بلکه بر سایر شاخص‌های کلیدی عملکرد در خصوص تجربه مشتری، مشارکت کارکنان و کارایی عملیاتی تمرکز کنند. سازمان‌ها می‌بایست برای به دست آوردن بینشی دقیق در مورد تأثیر تحولات دیجیتال و شناسایی زمینه‌های بهبود و بهینه‌سازی از تجزیه‌وتحلیل داده‌ها نیز استفاده کنند.

۱. Return on Investment

عنوان: Unleashing value from digital transformation: Paths and pitfalls
نویسنده: Tim Smith, Gregory Dost, Tim Bottke, Diana Kearns-Manolatos
مرکز مطالعاتی: Deloitte
تاریخ انتشار: January 31, 2023

رمزارزها، دلارهای دیجیتال و آینده پول

شورای روابط خارجی (CFR) مقاله‌ای تحت عنوان «رمزارزها، دلارهای دیجیتال و آینده پول» منتشر کرده است و در مورد تحولات پول و ظهور ارزهای دیجیتال، پیامدهای این اتفاق برای ثبات اقتصادی و مالی و چالش‌های نظارتی و ژئوپلیتیکی پیش رو بحث می‌کند. گزارش با بررسی تاریخچه پول، اشکال گوناگون آن و چگونگی تکامل آن در طول زمان آغاز شده و سپس به نحوه پیدایش ارزهای دیجیتال و رمزارزهای بانک مرکزی[۱] (CBDC) می‌پردازد که مدل دیجیتالی ارزهای فیات هستند و توسط بانک‌های مرکزی صادر شده و پشتیبانی می‌شوند. سپس تفاوت‌های بین رمزارزهای بانک مرکزی و ارزهای دیجیتال را شرح می‌دهد و مزایا و خطرات بالقوه رمزارزهای بانک مرکزی، همچون تأثیر آن‌ها بر واسطه‌گری مالی، سیاست‌های پولی و ثبات مالی را مورد بحث قرار می‌دهد. نویسندگان چالش‌های نظارتی ارزهای دیجیتال برای دولت‌ها و سیاست‌گذاران را بررسی می‌کنند. نیاز به یک رویکرد نظارتی متعادل که نوآوری را تقویت، از مصرف‌کنندگان محافظت و ثبات مالی را حفظ کند، از مواردی است که به آن‌ها اشاره شده است.

پیامدهای ژئوپلیتیکی افزایش ارزهای دیجیتال و تأثیر بالقوه ارزهای دیجیتال بر سیستم مالی جهانی، نقش ارزهای دیجیتال در تجارت بین‌المللی و پرداخت‌های فرامرزی و پتانسیل استفاده از ارزهای دیجیتال برای فعالیت‌های غیرقانونی مانند پول‌شویی و تأمین مالی تروریسم مورد بحث قرار می‌گیرد. بررسی پتانسیل ارزهای دیجیتال برای به چالش کشیدن تسلط دلار آمریکا در تجارت و امور مالی جهانی یکی از موضوعات مهمی است که به آن پرداخته می‌شود.

نویسندگان گزارش را با بحث در مورد آینده پول و پتانسیل ارزهای دیجیتال برای تغییر روش معامله و ذخیره ارزش به پایان می‌رسانند. نیاز به تحقیق و گفتمان مستمر میان سیاست‌گذاران، دانشگاهیان و ذی‌نفعان صنعت برای اطمینان از ادغام ارزهای دیجیتال در سیستم مالی جهانی به‌گونه‌ای که نوآوری، ثبات مالی و رشد اقتصادی را بیفزاید، از توصیه‌های آن‌ها است.

*

۱. central bank digital currencies (CBDCs)

عنوان	Cryptocurrencies, Digital Dollars, and the Future of Money
نویسنده	Anshu Siripurapu, Noah Berman
مرکز مطالعاتی	CFR
تاریخ انتشار	February 28, 2023

اتصال حیاتی:
کاهش قیمت داده در بازارهای آفریقا

گزارش «اتصال حیاتی: کاهش قیمت داده در بازارهای آفریقا» در آزمایشگاه تحقیقات قانونی دیجیتال شورای آتلانتیک (DFRLab) منتشر شده و به بررسی هزینه بالای داده‌های تلفن همراه در بازارهای آفریقا می‌پردازد و توصیه‌هایی را برای کاهش قیمت‌ها و بهبود دسترسی به اینترنت در این قاره ارائه می‌کند. این گزارش بر اهمیت دسترسی به اینترنت مقرون‌به‌صرفه در گره‌گشایی رشد اقتصادی و توسعه اجتماعی در آفریقا تأکید دارد.

علی‌رغم آن‌که هزینه داده‌های تلفن همراه در سطح جهانی کاهش یافته، بازارهای آفریقا همچنان قیمت‌های بالایی دارند، به‌طوری‌که میانگین قیمت ۱ گیگابایت داده ۷٫۱۲ درصد از درآمد ماهانه را دربر می‌گیرد. این رقم در اروپا تنها ۰٫۵۶ درصد است. این نابرابری، دسترسی به اطلاعات را محدود و از دسترسی کسب‌وکارهای آفریقایی به بازارهای جهانی جلوگیری کرده و مانع رشد اقتصادی این قاره می‌شود.

دلایل متعددی برای هزینه بالای داده‌ها در بازارهای آفریقا مورد شناسایی قرار گرفته است، ازجمله عدم رقابت بین اپراتورهای شبکه تلفن همراه، هزینه‌های بالای نظارتی و کمبود سرمایه‌گذاری در زیرساخت. مالیات‌ها و هزینه‌های تحمیل‌شده توسط دولت بر داده‌های تلفن همراه نیز این مشکلات را تشدید می‌کند، زیرا هزینه‌های ارائه خدمات داده را افزایش می‌دهد که در نهایت این هزینه‌ها به مصرف‌کنندگان منتقل می‌شود.

به منظور کاهش هزینه داده‌ها در بازارهای آفریقا پیشنهادات زیر توسط نویسنده گزارش مطرح می‌شود:

- افزایش رقابت بین اپراتورهای شبکه تلفن همراه از طریق کاهش موانع ورود و تشویق تازه‌واردان به این بازار؛
- ترویج سرمایه‌گذاری زیرساختی، به‌ویژه در مناطق روستایی برای گسترش پوشش و کاهش هزینه داده‌ها؛
- کاهش هزینه‌های نظارتی با ساده‌سازی فرایند صدور مجوز و ترویج نوآوری در این بخش؛
- کاهش مالیات‌ها و هزینه‌های تحمیلی دولت بر داده‌های تلفن همراه که هزینه ارائه خدمات داده و در نهایت قیمت‌ها را برای مصرف‌کنندگان کاهش می‌دهد.

در پایان ابتکارات موفقیت‌آمیزی که در بازارهای آفریقا برای کاهش هزینه داده اجرا شده است، مانند ابتکار اینترنت رایگان فیس‌بوک که دسترسی رایگان به مجموعه محدودی از خدمات اینترنتی را برای کاربران در برخی کشورها فراهم کرده، مورد بررسی قرار می‌گیرد. نویسنده به موفقیت اپراتورهای شبکه مجازی تلفن همراه (MVNO) در آفریقای جنوبی نیز اشاره می‌کند که باعث افزایش رقابت و کاهش قیمت‌ها در بازار شده است. طبق نتایج این گزارش کاهش هزینه داده‌ها در بازارهای آفریقا برای گره‌گشایی معضل رشد اقتصادی و توسعه اجتماعی در این قاره ضروری است و برای تحقق این امر، اتخاذ یک رویکرد چندجانبه با مشارکت دولت‌ها، اپراتورهای شبکه تلفن همراه، جامعه مدنی و سازمان‌های بین‌المللی پیشنهاد می‌شود.

عنوان	Critical connectivity: Reducing the price of data in African markets
نویسنده	Aubrey Hruby
مرکز مطالعاتی	Atlanticcouncil
تاریخ انتشار	March 3, 2023

راهکار جایگزین برای قانون ضدانحصار: پرداختن به مزیت رقابتی مضر

گزارش «راهکار جایگزین برای قانون ضد انحصار: پرداختن به مزیت رقابتی مضر» که توسط مؤسسه امریکن اینترپرایز منتشر شده است، رویکرد جدیدی را نسبت به مقررات ضدانحصار پیشنهاد می‌کند که به‌جای تمرکز بر قدرت بازار به مزیت‌های رقابتی مضر می‌پردازد. این گزارش تأکید می‌کند که هدف مقررات ضدانحصار باید ترویج رقابت و اطمینان از عملکرد بازارها به نفع مصرف‌کنندگان باشد، اما رویکرد ضدانحصار فعلی اغلب به تمرکز بازار می‌پردازد، امری که می‌تواند از نظر شناسایی رفتار مضر به شناسایی رفتار مثبت کاذب و رفتار منفی کاذب منجر شود. کلید شناسایی رفتار مضر تمرکز بر مزیت رقابتی است. مزیت رقابتی مثبت عبارت است از هر عاملی که به یک شرکت اجازه می‌دهد تا سود خود را از طریق رقابت برتر افزایش دهد و مزیت رقابتی مضر، هر مزیتی است که مبتنی‌بر عملکرد برتر نبوده و بر اساس رفتار ضد رقابتی یا شکست بازار است. این گزارش انواع مختلفی از مزیت‌های رقابتی مضر را برمی‌شمارد، ازجمله ثبت نظارتی، اثرات شبکه، مزایای داده و مالکیت معنوی. این مزایای منفی می‌تواند به رقابت و مصرف‌کنندگان آسیب برساند و باید موضوع تمرکز اصلی مقررات ضدانحصار باشد.

این گزارش برای پاسخگویی به این آسیب‌ها سیاست‌هایی را توصیه می‌کند. نخست، آژانس‌های ضدانحصار باید به تحقیق در صنایعی که خطر بالای مزیت رقابتی مضر دارند، بپردازند. دوم، آژانس‌های ضدانحصار باید به‌جای مجازات رفتار غیرقانونی پس از وقوع آن، به پیشگیری از آسیب بپردازند. اتخاذ یک رویکرد فعال‌تر برای شناسایی و رسیدگی به رفتار مضر ازجمله این اقدامات پیشگیرانه است. سوم، آژانس‌های ضدانحصار باید راه‌حل‌های مختلفی را فراتر از اقدامات اجرایی سنتی، راه‌حل‌های ساختاری، درمان‌های رفتاری و مداخلات نظارتی در نظر بگیرند.

این گزارش نقش نوآوری در رقابت و مقررات ضدانحصار را نیز بررسی می‌کند. نوآوری محرک اصلی رقابت است و مقررات ضدانحصار باید حامی نوآوری باشد نه مانع آن. آژانس‌های ضد انحصار باید رویکردی پویا نسبت به رقابت اتخاذ کنند که مزایای بالقوه نوآوری را در نظر گرفته و از سرکوب رقابت از طریق نظارت بیش‌ازحد جلوگیری کند.

عنوان	An Alternative Focus for Antitrust: Addressing Harmful Competitive Advantage
نویسنده	Mark Jamison
مرکز مطالعاتی	AEI
تاریخ انتشار	March 6, 2023

در میان اخراج‌های غول‌های فناوری، تقاضا برای کارگران خارجی دارای ویزای H-1B[1] هنوز هم بالاست

اندیشکده هریتیج گزارش «در میان اخراج‌های غول‌های فناوری، تقاضا برای کارگران خارجی دارای ویزای H-1B هنوز هم بالاست» را منتشر کرده است. این گزارش بر برنامه ویزای H-1B که به شرکت‌های آمریکایی اجازه می‌دهد تا به‌طور موقت کارگران خارجی با مهارت‌های تخصصی در مشاغلی مانند علوم، مهندسی و برنامه‌نویسی رایانه را استخدام کنند، تمرکز دارد و یادآوری می‌کند علی‌رغم اخراج کارکنان در برخی از بزرگ‌ترین شرکت‌های فناوری در ایالات‌متحده، تقاضا برای ویزای H-1B همچنان بالا است. درواقع، تعداد درخواست‌های ویزای H-1B در دهه گذشته همواره بالا بوده و سالانه صدها هزار درخواست ارسال می‌شود.

این مسئله گواهی بر «شکاف مهارت» در بازار کار ایالات‌متحده به‌ویژه در بخش فناوری است. شرکت‌های آمریکایی قادر به یافتن کارکنانی با مهارت‌های لازم برای پر کردن موقعیت‌های شغلی خود نیستند و برنامه ویزای H-1B منبع مهمی از استعداد برای شرکت‌های آمریکایی است. منتقدان اذعان می‌کنند شرکت‌ها از این برنامه برای استخدام کارکنان خارجی ارزان‌تر به‌جای شهروندان آمریکایی استفاده کرده‌اند و به فشار نزولی بر دستمزد کارگران در ایالات‌متحده دامن زده‌اند.

در مقابل موافقان معتقدند که این نگرانی‌ها اغراق‌آمیز بوده و برنامه ویزای H-1B درواقع برای کل اقتصاد ایالات‌متحده مفید است. این برنامه به شرکت‌های آمریکایی اجازه می‌دهد تا با دسترسی به بهترین استعدادها از سراسر جهان در بازار جهانی به رقابت بپردازد و برنامه فوق به پیشبرد نوآوری و رشد اقتصادی در ایالات‌متحده کمک می‌کند. بااین‌حال، ممکن است در برخی از زمینه‌ها اصلاحات در برنامه ویزای H-1B ضروری باشد. برای مثال، نویسنده پیشنهاد می‌کند که این برنامه می‌تواند به سمت مشاغلی که در آن شکاف مهارتی واقعی وجود دارد برود و بهتر مورد استفاده قرار گیرد و باید حمایت‌های قوی‌تری برای جلوگیری از سوءاستفاده کارفرمایان از برنامه فوق وجود داشته باشد.

۱. H-1B visa، این ویزا در واقع مجوزی است که توسط دولت ایالات متحده به یک تبعه خارجی برای کار در آمریکا داده می‌شود. تبعه خارجی باید در زمینه‌ای کار کند که نیاز به دانش تخصصی دارد. بنابراین این شخص، شرایط شغلی و مهارت‌هایی را انجام می‌دهد که کارفرما نتوانسته است در یک کارمند آمریکایی پیدا کند.

عنوان	Amid Big Tech Layoffs, Demand Still High for Foreign Workers With H-1B Visas. Something Doesn't Add Up.
نویسنده	Simon Hankinson
مرکز مطالعاتی	Heritage
تاریخ انتشار	March 6, 2023

چگونه سه ادغام موجب تقویت انحصار فناوری تبلیغات گوگل شد

گزارش «چگونه سه ادغام موجب تقویت انحصار فناوری تبلیغات گوگل شد» توسط اندیشکده سیاست فناوری و در مورد شکایت ضدانحصاری اخیر وزارت دادگستری ایالات‌متحده علیه گوگل است. این شکایت غول فناوری گوگل را به حفظ انحصار فناوری تبلیغاتی خود از طریق برخی ادغام‌ها و خریدهایی که رقبا را از بازار حذف کرده است، متهم می‌کند.

نویسنده در این خصوص به سه رفتار انحصارطلبانه و ادغام شرکت‌های متوسط به‌وسیله گوگل است. اولین مورد، خرید دابل کلیک[۱] در سال ۲۰۰۸ است؛ دابل کلیک یک پلتفرم تبلیغات دیجیتال بود که به گوگل اجازه داد تا به عنصری غالب در فضای تبلیغات آنلاین تبدیل شود. دومین مورد، خرید ادماب[۲] در سال ۲۰۱۰ بود، ادماب یک شبکه تبلیغات تلفن همراه بود که به گوگل کمک کرد تا بر بازار تبلیغات تلفن همراه تسلط یابد. سومین مورد، خرید لوکر [۳] در سال ۲۰۱۸ بود، لوکر یک پلتفرم تجزیه‌وتحلیل داده بود که به گوگل امکان ترکیب داده‌های تبلیغات خود با داده‌های مشتری را می‌داد تا تصویر جامع‌تری از رفتار مصرف‌کننده به دست بیاورد.

اکنون، وزارت دادگستری ایالات‌متحده اذعان می‌کند که رفتار ضدرقابتی گوگل باعث هزینه‌های تبلیغاتی بالاتر برای مشاغل و کاهش قدرت انتخاب مصرف‌کنندگان شده است. درآمد تبلیغات گوگل در سال ۲۰۲۱ حدود ۱۴۷ میلیارد دلار تخمین زده می‌شود که تقریباً ۲۸ درصد از بازار جهانی تبلیغات دیجیتال است. هدف این دعوا مجبور کردن گوگل به واگذاری برخی از دارایی‌های خود برای افزایش رقابت در بازار است.

صنعت فناوری تبلیغات بسیار پیچیده است و بازیگران زیادی ازجمله ناشران، تبلیغ‌کنندگان، پلتفرم‌های فناوری تبلیغات و کارگزاران داده را در برمی‌گیرد و مقررات‌گذاری به دلیل وابستگی متقابل بازیگران و سرعت بالای تغییرات فناورانه می‌تواند دشوار باشد. شکایت وزارت دادگستری علیه گوگل، گام مهمی در رسیدگی به موضوع انحصارطلبی در صنعت فناوری تبلیغات است؛ اما به نظر می‌رسد برای تضمین بازار رقابتی‌تر و عادلانه‌تر مقررات بیشتری مورد نیاز باشد و سیاست‌گذاران باید گزینه‌های زیادی، مانند مقررات حفظ حریم خصوصی داده‌ها، الزامات شفافیت و اجرای قوی‌تر قوانین ضدانحصاری را در نظر بگیرند.

۱. DoubleClick
۲. AdMob
۳. Looker

عنوان	How Three Mergers Buttressed Google's Ad Tech Monopoly, Per DOJ
نویسنده	Karina Montoya
مرکز مطالعاتی	Techpolicy
تاریخ انتشار	MArch 9, 2023

فروپاشی بخش فناوری آمریکا رخداد بدی خواهد بود

مؤسسه امریکن اینترپرایز (AEI) اخیراً در گزارشی تحت عنوان «فروپاشی بخش فناوری آمریکا رخداد بدی خواهد بود» به بررسی پیامدهای اقتصادی بالقوه مقررات ضدانحصار بر صنعت فناوری ایالات‌متحده می‌پردازد. اگرچه لازم است از عدم رفتار انحصاری شرکت‌ها یا مشارکت نداشتن آن‌ها در شیوه‌های ضدرقابتی اطمینان حاصل شود، اما باید توجه داشت که تنظیم‌گری شدید شرکت‌های فناوری پیامدهای اقتصادی منفی بیشتری خواهد داشت. این گزارش اثرات بالقوه این فرایند را بر نوآوری، قیمت نهایی مصرف‌کننده، ایجاد شغل و رقابت‌پذیری ایالات‌متحده بررسی می‌کند.

صنعت فناوری ایالات‌متحده مهم‌ترین محرک نوآوری این کشور است، به‌طوری‌که شرکت‌هایی مانند اپل، گوگل و مایکروسافت در شیوه زندگی و کار مردم انقلاب ایجاد کرده‌اند. این شرکت‌ها به دلیل سرمایه زیاد، بدون دخالت دولت توانسته‌اند به این نوآوری دست یابند و درحال حاضر اصرار بر تجزیه این غول‌های فناوری و افزایش خارج از قاعده قوانین ضدانحصاری، می‌تواند منجر به فروپاشی آن‌ها شود. فروپاشی شرکت‌های بزرگ فناوری می‌تواند به افزایش قیمت‌ها برای مصرف‌کنندگان بیانجامد، زیرا شرکت‌های کوچک‌تر توانایی صرفه‌جویی در مقیاس بالا یا قدرت چانه‌زنی با تأمین‌کنندگان را ندارند. افزایش مقررات ممکن است منجر به انتقال هزینه‌های اجرای مقررات، از شرکت‌ها به مصرف‌کنندگان شود.

از سوی دیگر، نگرانی‌هایی در مورد خطر بیکاری گسترده در صنعت فناوری وجود دارد که منبع اصلی رشد نرخ اشتغال‌آفرینی در ایالات‌متحده در سال‌های اخیر بوده است. فروپاشی یا تنظیم‌گری شدید شرکت‌های فناوری می‌تواند منجر به کاهش اشتغال‌آفرینی و رشد اقتصادی، به‌ویژه در مناطقی مثل دره سیلیکون شود که صنعت فناوری در آن محرک اصلی اقتصاد محلی است. بر همین اساس، اثرات بالقوه مقررات ضدانحصار بر رقابت‌پذیری ایالات‌متحده باید مورد ارزیابی قرار گیرند. صنعت فناوری ایالات‌متحده یک بازیگر بزرگ در سطح جهانی است و مقررات سنگین با فروپاشی شرکت‌های فناوری ایالات‌متحده می‌تواند منجر به از دست دادن این مزیت رقابتی در قبال کشورهای دیگر مانند چین شود. اگرچه مهم است از عدم وجود رفتار انحصارگرانه در شرکت‌های فناوری اطمینان حاصل شود، اما فروپاشی یا تنظیم شدید صنعت فناوری ایالات‌متحده پیامدهای اقتصادی منفی بیشتری خواهد داشت. در عوض سیاست‌گذاران باید بر اجرای هدفمند قوانین ضدانحصاری که به شیوه‌های خاص اقدامات ضدرقابتی می‌پردازد، تمرکز کنند تا مزایای صنعت فناوری پویا و نوآورانه نیز حفظ شود.

عنوان	Blowing Up the American Tech Sector Would be Bad
نویسنده	James Pethokoukis
مرکز مطالعاتی	AEI
تاریخ انتشار	March 13, 2023

بازخوردی به کمیسیون اروپا در خصوص شاخص‌های کلیدی عملکرد در دهه دیجیتال ۲۰۳۰

بنیاد فناوری اطلاعات و نوآوری (ITIF) گزارشی تحت عنوان «بازخوردی به کمیسیون اروپا در خصوص شاخص‌های کلیدی عملکرد در دهه دیجیتال ۲۰۳۰» منتشر کرده و شاخص‌های کلیدی عملکرد (KPI) پیشنهادی کمیسیون اروپا برای دهه دیجیتال ۲۰۳۰ را تحلیل نموده و در مورد زمینه‌هایی که نیازمند بهبود هستند، بازخوردهایی ارائه می‌دهد. نویسندگان با تأکید بر اهمیت دهه دیجیتال ۲۰۳۰ در پیشبرد تحولات دیجیتال اتحادیه اروپا و ارتقای نوآوری و رقابت، برای تعیین اهداف بلندپروازانه در زمینه مهارت‌های دیجیتال، اتصال و نوآوری از کمیسیون اروپا سپاس‌گزاری می‌کنند. بااین‌حال، نگرانی‌ها و مسائلی را نیز شناسایی کرده و توصیه‌هایی جهت بهبود ارائه می‌کنند.

یکی از این نکات کلیدی، نیاز به اتخاذ یک رویکرد جامع‌تر برای اندازه‌گیری پیشرفت در دستیابی به اهداف دهه دیجیتال ۲۰۳۰ است. شاخص‌های کلیدی عملکرد پیشنهادی کمیسیون اروپا بسیار محدود بوده و موارد زیادی از عوامل مؤثر بر تحول دیجیتال و نوآوری را در برنمی‌گیرند. کمیسیون اروپا باید شاخص‌های کلیدی عملکرد جامع‌تری را در نظر بگیرد و عواملی مانند سواد دیجیتال، ظرفیت نوآوری و توسعه اکوسیستم را حساب کند.

نیاز به تمرکز بیشتر بر توسعه مهارت‌های دیجیتال از دیگر موضوعاتی است که مورد بررسی قرار می‌گیرد. بر همین اساس، کمیسیون اروپا نیازمند آن است تا با توسعه مهارت‌های دیجیتال، برای افزایش سواد دیجیتالی در جامعه اتحادیه اروپا اهداف روشنی داشته باشد و برای توسعه و اجرای برنامه‌های آموزشی هماهنگ با نیازهای اقتصاد دیجیتال، با صنعت و مؤسسات آموزشی همکاری کند.

موضوع مهم دیگر، نیاز به سرمایه‌گذاری بیشتر در زیرساخت‌های دیجیتال است.کمیسیون اروپا برای بهبود اتصال دیجیتال در سراسر اتحادیه اروپا، به‌ویژه در مناطق روستایی و دورافتاده، باید اهداف روشنی داشته باشد و برای حمایت از توسعه خدمات و برنامه‌های کاربردی دیجیتال سرمایه‌گذاری در شبکه‌های پرسرعت پهن‌باند و زیرساخت 5G را مدنظر قرار دهد.کمیسیون اروپا برای افزایش سرمایه‌گذاری در تحقیق و توسعه (R&D) و ترویج رشد استارتاپ‌های نوآورانه و کسب‌وکارهای کوچک و متوسط نیز، باید اهداف مشخصی داشته باشد و برای ایجاد مکانیسم‌های تأمین مالی در مراحل اولیه از نوآوری حمایت کرده و منابعی را برای افزایش سرمایه‌گذاری‌های موفق گردآوری کرده و با صنعت و سرمایه‌گذاران همکاری کند.

در نهایت، این گزارش در مورد تأثیر بالقوه دهه دیجیتال ۲۰۳۰ بر حریم خصوصی و امنیت کاربران نگرانی‌هایی را عنوان می‌کند. ضروری است تا کمیسیون اروپا پیامدهای تحول دیجیتال بر حریم خصوصی و امنیت را به‌دقت بررسی نموده و برای رفع این نگرانی‌ها اقداماتی پیش گیرد. کمیسیون اروپا برای توسعه بهترین روش‌ها جهت حفاظت از داده‌ها و امنیت سایبری باید با صنعت و جامعه مدنی همکاری کند.

عنوان	Feedback to the European Commission on 2030 Digital Decade Key Performance Indicators
نویسنده	Kir Nuthi, Hodan Omaar, Patrick Grady
مرکز مطالعاتی	ITIF
تاریخ انتشار	March 10, 2023

اثرات ورود پلتفرم‌ها به بازار شخصی: شواهدی از بازار اپلیکیشن‌های موبایل

گزارش «اثرات ورود پلتفرم‌ها به بازار شخصی: شواهدی از بازار اپلیکیشن‌های موبایل» که توسط مؤسسه امریکن اینترپرایز (AEI) منتشر شده است، تأثیر ورود شرکت‌های مالک پلتفرم به بازارهای شخصی را بر رقابت و نوآوری در بازار اپلیکیشن‌های موبایل بررسی می‌کند. بر این اساس، با اینکه ورود شرکت‌های مالک پلتفرم به بازار شخصی ممکن است منجر به افزایش رقابت شود، پتانسیل آسیب به نوآوری و کاهش رفاه مصرف‌کننده را نیز در پی دارد. به همین منظور نویسندگان به بررسی بازار اپلیکیشن‌های موبایل تحت سلطه اپ‌استور اپل و پلی‌استور گوگل می‌پردازند. هر دو پلتفرم اپلیکیشن‌های خود را ارائه می‌دهند که با برنامه‌های شخص ثالث فروخته شده در بازارهای شخصی رقابت می‌کنند.

این گزارش تأثیر ورود پلتفرم‌ها به بازار شخصی را بر قیمت، کیفیت و نوآوری اپلیکیشن‌های خود و برنامه‌های شخص ثالث به‌خوبی تحلیل می‌کند. ورود شرکت‌های مالک پلتفرم به بازار شخصی می‌تواند منجر به افزایش رقابت و کاهش قیمت برای مصرف‌کنندگان شود. بااین‌حال، شرکت‌های مالک پلتفرم ممکن است به دلیل دسترسی به داده‌های کاربران نسبت به برنامه‌های شخص ثالث مزیت رقابتی داشته باشند که این امر می‌تواند منجر به کاهش نوآوری و کیفیت پایین‌تر برای مصرف‌کنندگان شود.

آسیب‌های احتمالی مرتبط با ورود شرکت‌های پلت فرم به بازار شخصی:

- شرکت‌های مالک پلتفرم می‌توانند برای اولویت دادن برنامه‌های کاربردی خود بر برنامه‌های شخص ثالث انگیزه قوی داشته باشند که این امر منجر به کاهش دید و قابلیت کشف برنامه‌های شخص ثالث می‌شود.
- شرکت‌های مالک پلتفرم ممکن است از کنترل خود بر داده‌های کاربران برای استفاده از برنامه‌های کاربردی خود استفاده کنند که این امر منجر به کاهش نوآوری و رقابت می‌شود.
- ورود شرکت‌های مالک پلتفرم به بازار شخصی ممکن است منجر به کاهش کیفیت برای مصرف‌کنندگان شود، چراکه توسعه‌دهندگان شخص ثالث اگر با برنامه‌های کاربردی شخصی پلتفرم‌ها مواجه شوند ممکن است انگیزه کمتری برای سرمایه‌گذاری در بهبود کیفیت اپلیکیشن خود داشته باشند.

نویسندگان به منظور جلوگیری از وقوع این آسیب‌ها برخی توصیه‌های سیاستی زیر را پیشنهاد می‌کند:

- آژانس‌های ضدانحصار باید بر ورود شرکت‌های پلتفرم به بازار شخصی کاملاً نظارت کنند تا از آسیب ندیدن رقابت و نوآوری اطمینان حاصل شود.
- پلتفرم‌ها باید اطلاعاتی را درباره نحوه استفاده از داده‌های کاربر برای اطلاع‌رسانی جهت توسعه برنامه‌های کاربردی خود افشا کنند تا از برابری پلتفرم‌ها و توسعه‌دهندگان شخص ثالث اطمینان حاصل شود.
- پلتفرم‌ها باید برای توسعه‌دهندگان شخص ثالث مشوق‌هایی جهت سرمایه‌گذاری در بهبود کیفیت در نظر بگیرند، مشوق‌هایی مانند ارائه سهم درآمد بالاتر برای برنامه‌های باکیفیت‌تر.

عنوان	Effects of Platforms' Entry into Own Marketplace: Evidence from the Mobile Application Market
نویسنده	Mark Jamison, Jakub Tecza, Peter Wang
مرکز مطالعاتی	AEI
تاریخ انتشار	March 6, 2023

روی دیگر سکه:
ریسک‌های مالی غیرقانونی در دارایی‌های مجازی

بنیاد دفاع از دموکراسی‌ها (FDD) گزارشی تحت عنوان «روی دیگر سکه: ریسک‌های غیرقانونی مالی در دارایی‌های مجازی» منتشر کرده است که به خطرات غیرقانونی مالی در خصوص دارایی‌های مجازی می‌پردازد و راه‌هایی را نشان می‌دهد که از طریق آن دارایی‌های مجازی، مانند ارزهای دیجیتال، می‌توانند برای مقاصد غیرقانونی همچون پول‌شویی، تأمین مالی تروریسم و سایر اشکال فعالیت‌های مجرمانه استفاده شوند.

دارایی‌های مجازی چالش‌های خاصی برای مؤسسات مالی سنتی و نهادهای نظارتی ایجاد می‌کنند، چراکه در پلتفرم‌های غیرمتمرکزی بکار می‌روند که امکان ناشناس ماندن و عدم نظارت را فراهم می‌کنند. این عدم نظارت موجب دشواری شناسایی فعالیت‌های غیرقانونی و جلوگیری از وقوع آن‌ها می‌شود.

یکی از یافته‌های مهم این گزارش آن است که استفاده از دارایی‌های مجازی برای فعالیت‌های غیرقانونی در حال ازدیاد است، مخصوصاً در مناطقی مانند آفریقا، آمریکای لاتین و جنوب شرقی آسیا که نظارت در آن‌ها ضعیف‌تر است. دارایی‌های مجازی می‌توانند برای سازمان‌های جنایی جذاب باشند، زیرا ناشناس می‌مانند و می‌توانند برای جابجایی مبالغ هنگفتی پول از مرزها با سهولت استفاده شوند.

نویسندگان راه‌های استفاده از دارایی‌های مجازی برای تأمین مالی تروریسم را برمی‌شمارند و به نمونه‌هایی چون استفاده امارت اسلامی از دارایی‌های مجازی برای تأمین مالی فعالیت‌های خود در سوریه و عراق اشاره می‌کنند. اگرچه استفاده از دارایی‌های مجازی برای تأمین مالی تروریسم در حال حاضر محدود است، اما پتانسیل تبدیل به تهدیدی بسیار بزرگ در آینده را دارد.

به‌منظور پاسخ به خطرات غیرقانونی از ناحیه دارایی‌های مجازی، سیاست‌های ذیل توصیه می‌شوند:

- **افزایش نظارت بر معاملات دارایی‌های مجازی**

نهادهای نظارتی باید برای ایجاد چارچوب‌هایی که به‌طور مؤثر فعالیت‌های غیرقانونی در فضای دارایی‌های مجازی را رصد و شناسایی می‌کنند، تلاش کنند.

- **لزوم افزایش همکاری‌های بین‌المللی در مبارزه با تأمین مالی غیرقانونی**

ماهیت دارایی‌های مجازی به‌گونه‌ای است که مرزهای جغرافیایی و قوانین سنتی را نادیده گرفته و به همین دلیل، همکاری بین‌المللی جهت جلوگیری از استفاده از آن‌ها برای فعالیت‌های غیرقانونی ضروری است.

- **افزایش آگاهی عمومی از خطرات مرتبط با دارایی‌های مجازی**

بسیاری از افراد و کسب‌وکارها ممکن است از خطرات بالقوه دارایی‌های مجازی بی‌اطلاع باشند و به همین خاطر، برای اطمینان از استفاده مسئولانه از آن‌ها نیاز به آموزش بیشتری احساس می‌شود.

عنوان	The Underside of the Coin: Illicit Finance Risks in Virtual Assets
نویسنده	Richard Goldberg, Alex Levitov
مرکز مطالعاتی	FDD
تاریخ انتشار	February 16, 2023

توسعه استانداردهای قابلیت همکاری سیستم‌ها برای ارزهای دیجیتال در گروه ۲۰

گزارش «توسعه استانداردهای قابلیت همکاری سیستم‌ها برای ارزهای دیجیتال در گروه ۲۰» تحلیلی از وضعیت کنونی مقررات ارزهای دیجیتال و نیاز به استانداردهای قابلیت همکاری سیستم‌ها در سطح بین‌المللی را بیان کرده و نقش گروه ۲۰ در توسعه این استانداردها را بررسی می‌کند. در ابتدا، نویسنده از ارزهای دیجیتال و مزایا و خطرات احتمالی آن یک نمای کلی ارائه کرده و وضعیت فعلی مقررات ارز دیجیتال و چالش‌های مرتبط با تنظیم این فناوری در حال تغییر را مورد بررسی قرار می‌دهد و اذعان می‌کند یک واکنش هماهنگ بین‌المللی نسبت به مقررات ارز دیجیتال نیاز است، زیرا داشتن رویکردهای نظارتی مختلف مانع از نوآوری و رشد می‌شود. گروه ۲۰ با درک نیاز به هماهنگی و همکاری بین‌المللی در این خصوص، فعالانه در مورد ارزهای دیجیتال مشارکت داشته است. در شرایط کنونی و تحت رهبری هند، گروه ۲۰ در ایجاد چارچوبی برای مقررات ارز دیجیتال که هم رافع نگرانی‌های مربوط به حمایت از مصرف‌کننده، ثبات مالی و فعالیت‌های غیرقانونی باشد و هم نوآوری را ترویج کند، فرصتی منحصربه‌فرد ارائه می‌کند. از همین رو، نویسنده توصیه‌هایی جهت توسعه استانداردهای قابلیت همکاری سیستم‌ها در ارزهای دیجیتال برای گروه ۲۰ ارائه می‌کند که در ادامه به آن‌ها اشاره خواهد شد.

- **ایجاد یک محیط قرنطینه نظارتی جهت نوآوری در ارز دیجیتال**

محیط قرنطینه نظارتی به توسعه‌دهندگان ارز دیجیتال اجازه می‌دهد محصولات و خدمات جدید خود را در محیطی کنترل‌شده آزمایش کنند و به تنظیم‌کنندگان فرصت می‌دهد تأثیر آن‌ها را بر سیستم مالی بزرگ‌تری نظارت و ارزیابی کنند.

- **ایجاد چارچوبی برای قابلیت همکاری سیستمی ارزهای دیجیتال**

استانداردهای قابلیت همکاری به ارزهای دیجیتال مختلف اجازه می‌دهد بدون نیاز به واسطه‌گری یا مبادلات پیچیده با هم کار کنند. این امر قابلیت استفاده و دسترسی ارزهای دیجیتال را می‌افزاید و آن‌ها را برای مصرف‌کنندگان و کسب‌وکارها جذاب‌تر می‌کند.

- **شفافیت و اشتراک‌گذاری اطلاعات در بین ذی‌نفعان**

اشتراک‌گذاری اطلاعات در مورد بهترین شیوه‌ها در خصوص وضع مقررات ارز دیجیتال و ترویج اشتراک‌گذاری داده‌ها در مورد تراکنش‌های ارز دیجیتال و تأثیر آن‌ها بر سیستم مالی منجر به افزایش نوآوری و سهولت در تنظیم‌گری ارزهای دیجیتال خواهد شد.

این گزارش بر اهمیت توسعه استانداردهای قابلیت همکاری برای ارزهای دیجیتال در سطح بین‌المللی تأکید می‌کند. گروه ۲۰ فرصتی عالی جهت ایجاد چارچوبی برای مقررات ارزهای دیجیتال است تا ضمن رفع مسائل مربوط به حمایت از مصرف‌کننده، ثبات مالی و فعالیت‌های غیرقانونی، نوآوری را بیفزاید. ذی‌نفعان با همکاری یکدیگر می‌توانند محیطی امن و مطمئن برای توسعه و استفاده از ارزهای دیجیتال ایجاد کرده و مطمئن باشند ارزهای دیجیتال به سیستم مالی فراگیرتر و پایدارتری کمک می‌کنند

عنوان	Beyond the Hype: Developing Interoperability Standards for Digital Currency at the G20
نویسنده	Antara Vats
مرکز مطالعاتی	ORFonline
تاریخ انتشار	February 3, 2023

ارزش پول: استبداد در کیف پول دیجیتال شما وجود خواهد داشت یا آزادی؟

گزارش «ارزش پول: استبداد در کیف پول دیجیتال شما وجود خواهد داشت یا آزادی؟» توسط مؤسسه امریکن اینترپرایز (AEI) منتشرشده و پیامدهای دیجیتالی شدن فزاینده پول را بر آزادی، حریم خصوصی و امنیت فردی بررسی می‌کند. به استدلال این گزارش با اینکه پرداخت‌های دیجیتال مزایای متعددی مانند افزایش کارایی و راحتی را ارائه می‌دهند، در صورت عدم تنظیم صحیح، خطرات قابل‌توجهی را برای آزادی و حریم خصوصی افراد ایجاد می‌کنند.

نویسندگان ابتدا چشم‌انداز فعلی پرداخت‌های دیجیتال را بررسی و یادآوری می‌کنند که استفاده از پول نقد فیزیکی در بسیاری از نقاط جهان به‌سرعت در حال کاهش است. آن‌ها سپس پیامدهای این تغییر را، ازجمله پتانسیل دولت‌ها و شرکت‌های خصوصی برای اعمال کنترل بیشتر بر تراکنش‌های مالی افراد، مورد بحث قرار می‌دهند و بر همین اساس، بر وضع مقرراتی برای حمایت از حقوق فردی و اطمینان از این‌که پرداخت‌های دیجیتال به‌جای تضعیف آزادی و حریم خصوصی، به ترویج آن می‌پردازد، تأکید می‌کنند. مقررات مؤثر باید به چندین موضوع کلیدی مانند حریم خصوصی داده‌ها، برخورداری از خدمات مالی، رقابت و ملاحظات سیاسی بپردازد.

- **حریم خصوصی**

حجم عظیم داده‌های تولیدشده در پرداخت‌های دیجیتال، کالاهایی ارزشمند هستند و دولت‌ها و شرکت‌های خصوصی ممکن است به دنبال جمع‌آوری و استفاده از این داده‌ها برای اهداف بسیاری ازجمله نظارت و تبلیغات هدفمند باشند، از این رو مقرراتی برای حافظت از حریم خصوصی داده‌های افراد و اطمینان از عدم سوءاستفاده از داده‌ها وضع شود.

- **برخورداری از خدمات مالی**

پرداخت‌های دیجیتال ممکن است نابرابری‌های موجود در برخورداری از خدمات مالی را تشدید کند. با اینکه پرداخت‌های دیجیتال می‌تواند دسترسی به خدمات مالی را افزایش دهد، نیازمند دسترسی به زیرساخت‌ها و دستگاه‌های دیجیتال نیز هست که می‌تواند برای بسیاری از افراد به‌ویژه در مناطق کم‌درآمد و روستایی دور از دسترس باشد. تنظیم‌کنندگان باید با ترویج توسعه زیرساخت‌های دیجیتال و اطمینان از دسترسی همه افراد به ابزارهای مورد نیاز، برای مشارکت در اقتصاد دیجیتال به این موضوع رسیدگی کنند.

- **رقابت**

تسلط تعداد کمی از شرکت‌های بزرگ در این بخش انتخاب مصرف‌کننده و نوآوری را محدود می‌کند. تنظیم‌کننده‌ها باید اقداماتی را برای ارتقای رقابت، مثلاً از طریق توسعه استانداردهای باز و ارتقای قابلیت همکاری بین سیستم‌های پرداخت دیجیتال مختلف، انجام دهند.

- **ملاحظات سیاسی**

در نهایت، این گزارش به پتانسیل پرداخت‌های دیجیتال برای استفاده بیشتر در اهداف سیاسی می‌پردازد، ازجمله استفاده از این فناوری توسط دولت‌هایی که به دنبال اعمال کنترل بیشتر بر شهروندان خود هستند. بر همین اساس، مقررات باید به شیوه‌ای تنظیم شوند که پرداخت‌های دیجیتال به‌جای تضعیف آزادی و حریم خصوصی افراد، آن را ترویج کند.

عنوان	?The Values of Money: Will Tyranny or Freedom Be in Your Digital Wallet
نویسنده	Jim Harper, J. Christopher Giancarlo
مرکز مطالعاتی	AEI
تاریخ انتشار	February 28, 2023

امنیت سایبری و جنگ اطلاعاتی

بازخوردی به کمیسیون اروپا در خصوص پیش‌نویس قانون تاب‌آوری سایبری

بنیاد فناوری اطلاعات و نوآوری (ITIF) گزارشی با عنوان «بازخوردی به کمیسیون اروپا در خصوص پیش‌نویس قانون تاب آوری سایبری» منتشر کرده است و به بررسی قانون پیشنهادی کمیسیون اروپا پرداخته و بر اهمیت آن در بهبود انعطاف‌پذیری سایبری اتحادیه اروپای در معرض تهدیدات سایبری، تأکید دارد.

یکی از نکات کلیدی این گزارش، نیاز به درک بهتر خطرات و آسیب‌پذیری‌ها در زیرساخت‌های حیاتی اتحادیه اروپا است. کمیسیون اروپا باید تحلیل جامعی از این خطرات و آسیب‌پذیری‌ها انجام دهد تا نقاط نیازمنده توجه، شناسایی شود. مضافاً کمیسیون باید حفاظت از زیرساخت‌های حیاتی مانند شبکه‌های انرژی و حمل‌ونقل را در اولویت قرار دهد.

نیاز به همکاری بیشتر بین کشورهای عضو اتحادیه اروپا در امر مبارزه با تهدیدات سایبری از دیگر نکات مهی است که به آن پرداخته می‌شود. کمیسیون اروپا باید برای کشورهای عضو چارچوبی در نظر گیرد تا اطلاعات مربوط به تهدیدهای سایبری را به اشتراک گذاشته و در اقدامات امنیت سایبری همکاری کنند. این چارچوب باید بر اساس بهترین شیوه‌ها بوده و حفاظت از زیرساخت‌های حیاتی را در اولویت قرار دهد. موضوع مهم دیگر، لزوم افزایش آگاهی و آموزش در مورد تهدیدات سایبری است. کمیسیون اروپا می‌بایست یک کمپین آگاهی عمومی برای آموزش شهروندان در مورد خطرات و آسیب‌پذیری‌های تهدیدات سایبری در نظر داشته و برای گنجاندن آموزش امنیت سایبری در برنامه‌های درسی با مؤسسات آموزشی همکاری کند.

در زمینه ضرورت پاسخگویی و اقدامات اجرایی ناظر بر آن به کمیسیون اروپا توصیه می‌شود تا برای عدم رعایت قانون، دستورالعمل‌ها و مجازات مشخصی در نظر بگیرد. مجازات‌ها باید متناسب با شدت تخلف بوده و به‌طور مستمر اجرا شوند. نویسنده نگرانی‌هایی در مورد تأثیر بالقوه قانون انعطاف‌پذیری سایبری بر نوآوری و رقابت نیز عنوان می‌کند. به توصیه او کمیسیون اروپا می‌بایست تأثیر این قانون بر اکوسیستم نوآوری اتحادیه اروپا را به‌دقت بررسی نموده و اقداماتی را برای کاهش اثرات منفی این قانون انجام دهد.

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

ناحیه‌موازی:
دفاع‌عمومی-خصوصی‌از‌محیط‌اطلاعاتی‌اوکراین

گزارش «ناحیه موازی: دفاع عمومی-خصوصی از محیط اطلاعاتی اوکراین» توسط شورای آتلانتیک منتشر شده و نقش مشارکت بخش عمومی و خصوصی در دفاع از محیط اطلاعاتی اوکراین در برابر کمپین‌های اطلاعات نادرست را موردبررسی قرار می‌دهد. با مرور نمای کلی از محیط اطلاعاتی اوکراین که از زمان الحاق کریمه در سال ۲۰۱۴ شدیداً مورد هدف کمپین‌های اطلاعات نادرست روسیه قرار گرفته است، به نظر می‌رسد که این کمپین‌ها بخشی از استراتژی گسترده روسیه برای تضعیف دموکراسی‌های غربی و پیگیری منافع خود است.

مشارکت بخش عمومی و خصوصی در دفاع از محیط اطلاعاتی اوکراین، می‌تواند از تخصص و منابع هر دو بخش استفاده کند و به راه‌حل‌های مؤثرتر و کارآمدتری منجر شوند. مشارکت دولتی و خصوصی می‌تواند به ایجاد اعتماد و همکاری بین ذی‌نفعان مختلف کمک کند، امری که برای دفاع اطلاعات موفق ضروری است. یک مثال قابل توجه از مشارکت بخش عمومی و خصوصی در عمل، تأسیس مرکز رسانه بحران اوکراین در سال ۲۰۱۴ برای مقابله با کمپین اطلاعات نادرست روسیه و آزمایشگاه تحقیقات قانونی دیجیتال برای شناسایی و افشای کمپین‌های اطلاعات نادرست است.

در این گزارش به نقش فناوری در دفاع از محیط اطلاعاتی نیز پرداخته شده است. فناوری می‌تواند ابزار قدرتمندی در تشخیص و مقابله با اطلاعات نادرست باشد، اما باید با تخصص و قضاوت انسانی استفاده شود. برخی فناوری‌های امیدوارکننده مانند یادگیری ماشینی و پردازش زبان طبیعی که برای کمک به تشخیص اطلاعات نادرست درحال‌توسعه هستند، باید مورد توجه قرار بگیرند.

نویسندگان به برخی از چالش‌ها و خطرات مرتبط با مشارکت عمومی-خصوصی در دفاع از محیط اطلاعاتی نیز می‌پردازند. این چالش‌ها شامل نگرانی در مورد پتانسیل سانسور و نیاز به ایجاد تعادل بین ملاحظات امنیتی و حفظ حریم خصوصی است. این چالش‌ها را می‌توان از طریق ساختارهای حکمرانی شفاف و پاسخ‌گو و تعهد به حمایت از آزادی بیان و حقوق بشر حل کرد.

عنوان	A parallel terrain: Public-private defense of the Ukrainian information environment
نویسنده	Emma Schroeder, Sean Dack
مرکز مطالعاتی	Atlanticcouncil
تاریخ انتشار	February 27, 2023

چگونه ناوگان ماهواره‌های خصوصی می‌تواند به تأمین امنیت آینده ارتش ایالات‌متحده کمک کند؟

این گزارش به مزایا و پتانسیل سامانه‌های ماهواره‌ای خصوصی برای ارتش ایالات‌متحده می‌پردازد. سیستم‌های ماهواره‌ای خصوصی می‌توانند نسبت به ماهواره‌های نظامی سنتی مزیت‌های قابل‌توجهی داشته باشد، مانند هزینه‌های کمتر، افزایش انعطاف‌پذیری و نوآوری بیشتر. سامانه‌های ماهواره‌ای خصوصی می‌توانند به رفع برخی از چالش‌های کلیدی پیش روی ارتش ایالات‌متحده، مانند زباله‌های فضایی و دخالت احتمالی قدرت‌های خارجی، کمک کنند. با توجه به وضعیت فعلی سیستم‌های ماهواره‌ای ارتش ایالات‌متحده، این کشور دارای شبکه بزرگ و پیچیده‌ای از ماهواره‌های نظامی است، اما این سیستم‌ها شدیداً در برابر تهدیدات سایر کشورها، به‌ویژه چین و روسیه، آسیب‌پذیر هستند.

سیستم‌های ماهواره‌ای خصوصی می‌توانند انعطاف‌پذیری و نوآوری بیشتری داشته باشند، زیرا شرکت‌های خصوصی می‌توانند به نیازهای در حال تغییر فناوری و عملیاتی سریع‌تر پاسخ دهند. شرکت‌های خصوصی هزینه‌های کمتری دارند، زیرا مثل ارتش تحت فرایندهای تدارکاتی و موانع اداری نیستند. آن‌ها می‌توانند ماهواره‌های کوچک‌تر و چابک‌تری را مستقر کنند و کمتر به مشکل رو به رشد زباله‌های فضایی دامن بزنند. شرکت‌های خصوصی امکان توسعه فناوری‌هایی را دارند که کمتر در معرض مداخله قدرت‌های خارجی است، زیرا مثل سیستم‌های نظامی مشمول الزامات و محدودیت‌های امنیتی نیستند.

این گزارش با بحث در مورد برخی از چالش‌ها و خطرات مرتبط با سیستم‌های ماهواره‌ای خصوصی، مانند خطرات احتمالی امنیت سایبری و نگرانی در مورد مالکیت و کنترل خارجی، به پایان می‌رسد. ارتش ایالات‌متحده در شرایطی کنونی نیازمند آن است تا با استفاده از تخصص و منابع شرکت‌های خصوصی به تأمین امنیت آینده خود در یک محیط فضایی شدیداً چالش‌برانگیز کمک کند. به منظور دستیابی به این هدف، باید به ریسک‌ها و چالش‌های بالقوه سیستم‌های ماهواره‌ای خصوصی توجه دقیقی شود و نظارت و همکاری بین شرکت‌های خصوصی و ارتش امریکا برای تضمین موفقیت آن‌ها ضروری است.

“

عنوان	How a fleet of private satellites can help secure the US military's future
نویسنده	Aidan Poling
مرکز مطالعاتی	Atlanticcouncil
تاریخ انتشار	February 27, 2023

هفت دیدگاه در مورد گسترش قابلیت‌های سایبری تهاجمی

گزارش «ساختن بازار: هفت دیدگاه در مورد گسترش قابلیت‌های سایبری تهاجمی» از شورای آتلانتیک در مورد فراگیری روزافزون قابلیت‌های سایبری تهاجمی و چگونگی تأثیر این گسترش بر امنیت جهانی بحث کرده هفت دیدگاه از کارشناسان دانشگاه، صنعت و دولت را به‌منظور ارائه درک جامعی از وضعیت فعلی بررسی می‌کند.

این گزارش ابتدا به ماهیت در حال تحول درگیری سایبری و چگونگی تغییر آن از حالت دفاعی به حالت تهاجمی می‌پردازد. **توسعه قابلیت‌های تهاجمی اغلب توسط عوامل دولتی انجام می‌شود که به دنبال کسب مزیت استراتژیک هستند، اما مرز بین بازیگران دولتی و غیردولتی شدیداً کمرنگ می‌شود.**

دیدگاه دوم به بررسی راه‌هایی می‌پردازد که از طریق آن گسترش قابلیت‌های سایبری تهاجمی بر چشم‌انداز امنیت بین‌المللی تأثیر گذاشته است. **افزایش دسترسی به این قابلیت‌ها منجر به کم شدن بازدارندگی و افزایش خطر رشد قابلیت‌های تهاجمی سایبری شده است.**

دیدگاه سوم به بررسی نقش بیمه سایبری در ایجاد انگیزه برای توسعه قابلیت‌های تهاجمی می‌پردازد. **دسترسی به بیمه حملات سایبری می‌تواند منجر به تشکیل بازاری برای قابلیت‌های تهاجمی شود، زیرا شرکت‌های بیمه ممکن است مایل باشند برای دسترسی به این قابلیت‌ها به‌منظور کاهش ریسک خود هزینه بپردازند.**

دیدگاه چهارم در مورد نقش بخش خصوصی در گسترش قابلیت‌های تهاجمی است. **توسعه این قابلیت‌ها در شرکت‌های خصوصی می‌تواند موجب شرایطی شود تا انگیزه مالی بر ملاحظات امنیت ملی غلبه کند.**

دیدگاه پنجم پتانسیل قابلیت‌های سایبری تهاجمی برای استفاده در جنگ ترکیبی را بررسی می‌کند. **این قابلیت‌ها می‌تواند برای پشتیبانی از عملیات نظامی متعارف یا ایجاد اختلال در زیرساخت‌های حیاتی مورد استفاده قرار گیرد که این امر می‌تواند در برابر کشورهایی که به‌شدت متکی به فناوری هستند مؤثر باشد.**

دیدگاه ششم پتانسیل قابلیت‌های تهاجمی سایبری برای استفاده در زمینه جاسوسی بین‌المللی را مورد بررسی قرار می‌دهد. **توانایی اجرای عملیات جاسوسی سایبری در مقیاس بزرگ می‌تواند به دولت‌ها اجازه دهد تا اطلاعات حساس را بدون نیاز به روش‌های سنتی جمع‌آوری اطلاعات جمع‌آوری کنند.**

دیدگاه آخر به بررسی پیامدهای قابلیت‌های سایبری تهاجمی برای آینده کنترل تسلیحات می‌پردازد. **گسترش این قابلیت‌ها ممکن است مذاکره درباره توافق‌نامه‌های کنترل تسلیحات را دشوار کند، زیرا تأیید تطبیق با چنین توافق‌هایی می‌تواند دشوار باشد.**

به‌طورکلی، این گزارش مروری جامع از مسائل پیچیده گسترش قابلیت‌های تهاجمی سایبری ارائه می‌کند. نویسندگان بر نیاز به یک پاسخ هماهنگ بین‌المللی تأکید داشته و ادعا می‌کنند که شفافیت و گفت‌وگوی بین دولت‌ها برای کاهش خطرات مرتبط با این روند ضروری است.

عنوان	Makings of the Market: Seven perspectives on offensive cyber capability proliferation
نویسنده	Winnona DeSombre-Bernsen, Sophia D'Antoine, Daniel Moore, Christopher Bing, Ollie Whitehouse, Monica Ruiz, Jen Roberts
مرکز مطالعاتی	Atlanticcouncil
تاریخ انتشار	March 1, 2023

تقویت پیوند فناوری و امنیت ملی بریتانیا

گزارش «تقویت پیوند فناوری و امنیت ملی بریتانیا» به بررسی چالش‌های بریتانیا در تأمین امنیت ملی خود در عصر دیجیتال پرداخته و گوشزد می‌کند، پیشرفت‌های فناوری تهدیدات جدید و پیچیده‌ای برای امنیت ملی آفریده است، تهدیداتی چون حملات سایبری، کمپین‌های اطلاعات نادرست و مسلح سازی[۱] فناوری‌های نوظهوری چون هوش مصنوعی. مضافاً، قابلیت دولت بریتانیا در پاسخگویی به این تهدیدها به دلیل فقدان سرعت و نوآوری در دستگاه امنیت ملی این کشور مانع بزرگی است.

گزارش فوق برای پرداختن به این چالش‌ها پیشنهاد می‌کند دولت بریتانیا بر سه حوزه کلیدی نوآوری، همکاری و مقررات تمرکز کند. در خصوص نوآوری، دولت باید روی فناوری‌های نوظهور سرمایه‌گذاری نموده و با بخش خصوصی همکاری نزدیک‌تری داشته باشد تا از همگامی با آخرین پیشرفت‌ها اطمینان حاصل شود. با توجه به ماهیت فراملی بسیاری از تهدیدات پیش روی بریتانیا همکاری ادارات مختلف دولتی و شرکای بین‌المللی نیز بسیار مهم است. در پاسخ به نیاز مقررات بیشتر و مؤثرتر در حوزه فناوری، دولت باید در تعیین استانداردهای امنیت سایبری و حفاظت از زیرساخت‌های حیاتی ملی رویکرد فعال‌تری اتخاذ کند و تعامل خود با شرکت‌های فناوری را افزایش دهد و آن‌ها را تشویق کند تا رویکرد مسئولانه‌تری در قبال محصولات و خدمات خود داشته باشند.

در پایان، به اعتقاد نویسندگان دولت بریتانیا باید استراتژی منسجم‌تر و هماهنگ‌تری برای امنیت ملی در عصر دیجیتال ایجاد کند. رویکرد کنونی دولت پراکنده و فاقد رهبری مشخص است و در نتیجه نمی‌تواند از قابلیت‌های فناوری‌های نوظهور به‌طور کامل استفاده کند و کشور را در معرض تهدیدهای جدید و پیچیده قرار می‌دهد.

۱. weaponization

عنوان	Strengthening the Link Between Technology and UK National Security
نویسنده	Joseph Jarnecki, Pia Husch
مرکز مطالعاتی	Rusi
تاریخ انتشار	March 2, 2023

بازنویسی پیمان امنیت سایبری دولت ایالات‌متحده و بخش خصوصی

گزارش جدید مرکز ویلسون با عنوان «بازنویسی پیمان امنیت سایبری دولت ایالات‌متحده و بخش خصوصی» وضعیت فعلی امنیت سایبری در ایالات‌متحده را که در آن بخش خصوصی، در عین آسیب‌پذیری در برابر حملات سایبری، مالک و اداره‌کننده بسیاری از زیرساخت‌های حیاتی بوده را نمایان کرده و اتخاذ یک رویکرد مشترک برای امنیت سایبری بین دولت ایالات‌متحده و بخش خصوصی را یک امر ضروری می‌داند. چراکه با وجود تلاش‌های بسیار دولت جهت افزایش امنیت سایبری، این حملات همچنان آسیب‌های اقتصادی و اجتماعی بسیاری ایجاد می‌کنند.

در طول سال‌های اخیر و با افزایش شدت و دامنه حملات سایبری، رویکرد سنتی «کاربر مراقب» که در آن بخش خصوصی مسئول ایمن‌سازی سیستم‌های خود است، در مواجهه با تهدیدات سایبری پیچیده و مداوم دیگر کارایی ندارد. در عوض، سیاست‌گذاران امنیت سایبری باید توجه خود را معطوف به رویکرد جدیدی کنند که حامی همکاری بین دولت و سازمان‌های بخش خصوصی است.

اصولی که از طریق آن دولت می‌تواند سطح همکاری را افزایش دهد عبارت‌اند از:

- افزایش اشتراک‌گذاری اطلاعات؛
- ارتقای استانداردهای امنیت سایبری؛
- ایجاد واکنش‌های هماهنگ به حوادث سایبری.

البته باید توجه داشت که دولت می‌تواند برای استفاده از بخش خصوصی در راستای افزایش امنیت سایبری از منابع و تخصص خود استفاده کند و این بار را بر دوش سازمان‌ها نگذارد. نکته مهم دیگر در این رویکرد جدید، نیاز به ایجاد انتظارات و رهنمودهای مشخص هم برای دولت و هم برای سازمان‌های بخش خصوصی است. دولت باید راهنمایی‌های واضحی ارائه کند تا مشخص شود مسئول دفاع در برابر چه نوع تهدیدات سایبری است و می‌تواند چه نوع حمایتی از بخش خصوصی کند. سازمان‌های بخش خصوصی نیز باید ملزم به اجرای حداقل میزان کنترل‌های امنیت سایبری شده و حوادث سایبری را به سرعت به دولت گزارش کنند. اتخاذ رویکردی هماهنگ‌تر و منسجم‌تر در خصوص امنیت سایبری در همه سازمان‌های دولتی ضروری است. دولت برای نظارت بر سیاست امنیت سایبری و هماهنگی واکنش‌ها به حوادث سایبری باید یک مرجع مرکزی در نظر بگیرد و برای کاهش بار نظارتی بر سازمان‌های بخش خصوصی، باید با تلفیق مقررات امنیت سایبری و ساده‌سازی الزامات انطباق تلاش کند.

عنوان	No More "User Beware": Rewriting the Cybersecurity Pact Between the US Government and Private Sector
نویسنده	Mary Brooks
مرکز مطالعاتی	Wilsoncenter
تاریخ انتشار	March 3, 2023

مروری بر سند دیدامنیت سایبری آمریکا

بنیاد دفاع از دموکراسی‌ها(FDD) گزارشی تحت عنوان «ما یک استراتژی جدید امنیت ملی سایبری داریم. حالا چه؟» منتشر کرده و به تحلیل سند اخیر استراتژی ملی سایبری ۲۰۲۳ که توسط دولت بایدن منتشر شده می‌پردازد. این استراتژی توسط کمیسیون سولاریوم فضای سایبری[۱] با هدف پاسخگویی به اهداف عملیاتی همچون بهبود انعطاف پذیری زیرساخت، افزایش همکاری میان بخش عمومی و خصوصی، سرمایه‌گذاری در امنیت شبکه فناوری اطلاعات فدرال، ایمن‌سازی اکوسیستم سایبری، تحمیل هزینه بر بازیگران متخاصم و توسعه قابلیت‌های سایبری شرکای بین‌المللی تدوین شده است.

با توجه به چالش‌های کنونی زیرساخت‌های حیاتی ایالات متحده آمریکا، این استراتژی تنظیم دستورالعمل امنیت سایبری برای صنایع فاقد دستورالعمل‌های خاص را پیشنهاد می‌کند. این امر، سردرگمی حاکم بر نظام امنیت سایبری آمریکا را تصدیق کرده و هدف از استراتژی جدید نیز، بهبود وضعیت موجود و هماهنگ‌سازی مقررات برای پشتیبانی از زیرساخت است.

این گزارش بر اهمیت مواردی چون تلاش برای مدرن‌سازی زیرساخت‌های فناوری اطلاعات فدرال، ایجاد شبکه واکنش به حوادث سایبری و ارتقای هنجارهای بین‌المللی و همکاری در فضای سایبری تأکید دارد و حوزه‌هایی را که در آن استراتژی ناکافی بوده است، شناسایی می‌کند؛ به عنوان مثال، این استراتژی می‌توانست به‌طور صریح‌تری به تهدیدات ناشی از حملات باج‌افزاری بپردازد و در مورد برنامه‌ریزی دولت فدرال جهت همکاری با شرکای خصوصی برای جلوگیری و پاسخ به چنین حملاتی جزئیات بیشتری در اختیار قرار دهد.

۱. the Cyberspace Solarium Commission

استراتژی جدید به موضوع پیام‌رسان‌های رمزگذاری شده اعتنا نمی‌کند و در عوض خواستار همکاری بیشتر بین صنعت و دولت برای افزایش امنیت دیجیتال است. این سیاست برای مقابله با چالش سرویس‌های پیام‌رسانی رمزگذاری‌شده که ممکن است توسط سازمان‌های جنایی و گروه‌های تروریستی برای برقراری ارتباط امن مورد استفاده قرار گیرند، کافی نیست. نگرانی دیگر، نیاز دولت فدرال به افزایش سرمایه‌گذاری در حوزه تحقیق و توسعه امنیت سایبری است. این استراتژی مستلزم افزایش بودجه در نوآوری‌های امنیت سایبری است. این گزارش نشان می‌دهد دولت فدرال باید از تحقیقات نوآورانه‌ای که می‌تواند به دفاع در برابر تهدیدات نوظهور کمک کند، حمایت بیشتری انجام دهد. در نتیجه، اگرچه استراتژی سایبری ملی ۲۰۲۳ یک گام مثبت و روبه‌جلو است، هنوز برای محافظت از زیرساخت‌های دیجیتال کشور و حفاظت از بعد سایبری امنیت ملی کارهای زیادی برای انجام وجود دارد.

عنوان	?We Have a New National Cybersecurity Strategy. Now What
نویسنده	RADM (Ret) Mark Montgomery, Samantha Ravich
مرکز مطالعاتی	FDD
تاریخ انتشار	March 3, 2023

ابعاد سایبری درگیری روسیه و اوکراین

مؤسسه بین‌المللی مطالعات استراتژیک[۱] در گزارشی ابعاد سایبری درگیری روسیه و اوکراین را بررسی کرده است. این گزارش نشان می‌دهد که چگونه جنگ با استفاده از حملات سایبری و اطلاعات نادرست در کنار تاکتیک‌های نظامی سنتی تبدیل به نوع جدیدی از جنگ تلفیقی شده است. این مطالعه اذعان می‌کند استفاده از حملات سایبری پتانسیل تشدید درگیری و ایجاد خسارت قابل‌توجه به هر دو طرف را دارد.

روسیه و اوکراین هر دو قابلیت‌های سایبری قابل‌توجهی را توسعه داده و از این قابلیت‌ها در درگیری‌های جاری استفاده کرده‌اند. عملیات سایبری روسیه بر کمپین‌های اطلاعات نادرست، هدف قرار دادن زیرساخت‌های نظامی و غیرنظامی اوکراین و انجام فعالیت‌های شناسایی و جاسوسی پایه‌گذاری شده است. اوکراین در کنار ایجاد قابلیت‌های سایبری، اقداماتی را به منظور تمرکز بر حفاظت از زیرساخت‌های حیاتی خود و هدف قرار دادن عملیات روسیه نیز به انجام رسانده است.

جنگ میان این دو کشور، نشان داد که استفاده از قابلیت‌های سایبری در درگیری، پتانسیل تشدید و ایجاد خسارات قابل‌توجهی را دارد. حملات سایبری توانایی ایجاد اختلال در زیرساخت‌های حیاتی و اختلالات اقتصادی و اجتماعی بسیاری را دارند. مضافاً، حملات سایبری پتانسیل بالایی در ایجاد سردرگمی از طریق اطلاعات نادرست دارد بدین‌صورت که تشخیص وضعیت واقعی میدان نبرد را برای هر دو طرف دشوار می‌کند.

امروزه استفاده از قابلیت‌های سایبری بخشی جدایی‌ناپذیر از جنگ مدرن شده و احتمالاً در درگیری‌های آینده بیشتر هم خواهد شد. در نتیجه برای کنترل استفاده از قابلیت‌های سایبری در درگیری‌ها باید بر اهمیت هنجارها و توافق‌های بین‌المللی تأکید داشت. جامعه بین‌المللی باید بر ایجاد چارچوبی برای رفتار مسئولانه در فضای سایبری مبادرت کند.

از سوی دیگر، جنگ میان اوکراین و روسیه حاکی از اهمیت حفاظت از زیرساخت‌های حیاتی در برابر حملات سایبری است. دولت‌ها و نهادهای بخش خصوصی باید در اقدامات امنیت سایبری برای محافظت از زیرساخت‌های حیاتی خود در برابر حملات سایبری سرمایه‌گذاری کنند. به توصیه این گزارش دولت‌ها باید برای توسعه یک رویکرد جامع برای حفاظت از زیرساخت‌های حیاتی در برابر حملات سایبری با یکدیگر همکاری کنند.

۱. The International Institute for Strategic Studies (IISS)

عنوان	The Cyber Dimension of the Russia Ukraine War
نویسنده	Marcus Willett
مرکز مطالعاتی	IISS
تاریخ انتشار	March 6, 2023

مدیریت مبارزه با اخبار جعلی

گزارش «مدیریت مبارزه با اخبار جعلی » به بررسی چالش‌های کمپین‌های اخبار جعلی وجود پرداخته و برای دولت‌ها و سازمان‌های جامعه مدنی توصیه‌هایی جهت مبارزه با آن ارائه می‌کند. اخبار جعلی تهدیدی اساسی علیه دموکراسی هستند که اعتماد به نهادهای عمومی را تضعیف کرده و در بسیاری از مواقع، این دروغ‌ها ممکن است پیامدهایی واقعی داشته باشد. پاسخ به کمپین‌های اخبار جعلی نیازمند رویکردی جامع و مشارکتی و طیفی از بازیگران همچون دولت‌ها، سازمان‌های جامعه مدنی، رسانه‌ها و پلتفرم‌های رسانه‌های اجتماعی است. اقدامات متقابل برای اثرگذاری تنها نیازمند شناسایی و حذف اخبار جعلی نیست، بلکه به ارتقای اطلاعات دقیق و تولید برنامه‌های سواد دیجیتالی برای کمک به افراد به‌منظور شناسایی و ارزیابی صحت اطلاعات آنلاین نیز نیاز دارد. همکاری‌های بین‌المللی نیز امکان اثرگذاری بالایی در مبارزه با اخبار جعلی دارد، چراکه اکثر کمپین‌های اخبار جعلی اغلب ابعاد بین‌المللی داشته و به همکاری دولت‌ها و سازمان‌های جامعه مدنی از چندین کشور برای خنثی‌سازی احتیاج دارند. به همین دلیل، افزایش همکاری و هماهنگی بین کشورها برای اشتراک‌گذاری بهترین روش‌ها و هماهنگی پاسخ به کمپین‌های اخبار جعلی امری ضروری است.

این گزارش توصیه‌هایی را برای دولت‌ها و سازمان‌های جامعه مدنی جهت مبارزه با اخبار جعلی نیز ارائه می‌کند. این توصیه‌ها شامل توسعه سیستم‌های هشدار اولیه برای شناسایی کمپین‌های احتمالی اخبار جعلی، اتخاذ ابتکارات حقیقت‌سنجی جهت ارتقای اطلاعات دقیق و تولید برنامه‌های مربوط به ارتقای سواد دیجیتال جهت کمک به افراد برای شناسایی و ارزیابی صحت اطلاعات آنلاین است. پلتفرم‌های رسانه‌های اجتماعی نیز نقشی کلیدی در مبارزه با اطلاعات نادرست دارند. پلتفرم‌ها باید فعالانه برای شناسایی و حذف اخبار جعلی اقدام کرده و با دولت‌ها و سازمان‌های جامعه مدنی برای توسعه و اجرای اقدامات متقابل مؤثر همکاری کنند.

عنوان	Managing to Fight Disinformation
نویسنده	Michael Khoo
مرکز مطالعاتی	Techpolicy
تاریخ انتشار	MArch 6, 2023

استارلینک و جنگ روسیه و اوکراین

گزارش «استارلینک و جنگ روسیه و اوکراین: پرونده‌ای برای فناوری تجاری و اهداف عمومی» در مرکز علوم و امور بین‌الملل بلفر در دانشگاه هاروارد منتشرشده و به بررسی نقش فناوری ماهواره‌ای تجاری در درگیری روسیه و اوکراین و به‌طور خاص در سرویس اینترنت ماهواره‌ای استارلینک می‌پردازد.

این گزارش تاریخچه‌ای درباره درگیری‌های کنونی روسیه و اوکراین و اهمیت فناوری ماهواره‌ای در جنگ‌های مدرن ارائه نموده و سپس سرویس استارلینک و قابلیت آن را برای متحول کردن بازار اینترنت ماهواره‌ای با تأخیر کم و قابلیت‌های پهنای باند بالا معرفی می‌کند. سپس به تحلیل پیامدهای احتمالی استقرار استارلینک در درگیری‌های اوکراین پرداخته و یادآوری می‌کند فناوری‌های ماهواره‌ای نقشی کلیدی در این درگیری‌ها داشته است، زیرا روسیه و اوکراین برای مقاصد شناسایی و ارتباطی از ماهواره‌ها استفاده می‌کنند؛ اما قابلیت‌های منحصربه‌فرد استارلینک می‌تواند به ایالات‌متحده و متحدانش مزیت‌های قابل‌توجهی در درگیری‌ها ببخشد.

برخی مزایای کلیدی استارلینک برای اهداف نظامی و اطلاعاتی عبارت‌اند از:

- تأخیر کم و قابلیت‌های پهنای باند بالا استارلینک را برای ارتباطات فوری و انتقال داده ایده‌آل می‌کند. این امر می‌تواند برای عملیات نظامی و جمع‌آوری اطلاعات در مناطق دورافتاده اوکراین که زیرساخت‌های ارتباطی سنتی آن محدود است، مفید باشد.
- پوشش جهانی استارلینک می‌تواند جایگزین مطمئن‌تر و قابل‌اعتمادتری برای شبکه‌های ارتباطی ماهواره‌ای موجود باشد که در برابر مداخلات و هک آسیب‌پذیر هستند.
- ماهیت تجاری استارلینک به گونه‌ای است که مانند ماهواره‌های دولتی مشمول محدودیت‌ها و مقررات حقوق بین‌الملل نشده و به ایالات‌متحده و متحدانش در نحوه استفاده از این فناوری انعطاف می‌دهد.

بااین‌حال، خطرات و چالش‌های مرتبط با استفاده از استارلینک در درگیری‌ها نیز باید مورد توجه قرار گیرند. یکی از ریسک‌های اساسی این است که روسیه استارلینک را یک تهدید تلقی کند و با اقدامات متقابل پاسخ دهد؛ این امر به‌طور بالقوه منجر به تشدید درگیری‌ها می‌شود. چالش دیگر اطمینان از استفاده از این فناوری به‌گونه‌ای است که با قوانین و هنجارهای بین‌المللی سازگار باشد. این امر نیاز به بررسی دقیق مسائلی چون اصول حاکم بر نظام حقوق بین‌الملل، حریم خصوصی، امنیت داده‌ها و حفاظت از غیرنظامیان دارد.

برای رسیدگی به خطرات و چالش‌های فوق، توصیه‌های زیر مطرح می‌شوند:

مشارکت میان بخش دولتی و خصوصی، به منظور حصول اطمینان از به کارگیری استارلینک در راستای منافع عمومی. چنین مشارکتی می‌تواند سازمان‌های دولتی، شرکت‌های خصوصی و جوامع مدنی را درگیر کند که با یکدیگر همکاری کنند و دستورالعمل‌هایی را برای استفاده از فناوری توسعه دهند و از استقرار و سازگاری این فناوری با قوانین و هنجارهای بین‌المللی اطمینان حاصل کنند.

تعامل با روسیه و سایر دشمنان بالقوه جهت ارتقای شفافیت و کاهش خطر سوءتفاهم یا اشتباه محاسباتی. این مهم می‌تواند از طریق اشتراک‌گذاری اطلاعات در مورد قابلیت‌ها و استفاده‌های موردنظر از استارلینک و سایر فناوری‌های ماهواره‌ای و بررسی فرصت‌های همکاری در مورد موضوعاتی مانند کاهش زباله‌های فضایی اتفاق بیفتد.

سرمایه‌گذاری در تحقیق و توسعه جهت بهبود قابلیت‌های فناوری ماهواره‌ای برای اهداف نظامی و اطلاعاتی. توسعه حسگرها و فناوری‌های ارتباطی جدید که می‌توانند در محیط‌های جنگی عمل کرده و امنیت سایبری و قابلیت‌های تجزیه‌وتحلیل داده‌ها را بهبود بخشند، ازجمله این موارد است.

عنوان	Starlink and the Russia-Ukraine War: A Case of Commercial Technology and Public Purpose?
نویسنده	Amritha Jayanti
مرکز مطالعاتی	Belfercenter
تاریخ انتشار	March 9, 2023

جنگ روسیه علیه اوکراین: تسریع تکه‌تکه شدن اینترنت

این گزارش به بررسی تأثیر جنگ بین روسیه و اوکراین بر تکه‌تکه شدن اینترنت پرداخته است. این گزارش نمایی کلی از تأثیر این جنگ بر اینترنت اوکراین و روسیه و پیامدهای ژئوپلیتیکی گسترده‌تر این تجزیه را نمایش می‌دهد.

حمله نظامی روسیه به خاک اوکراین از چند بابت منجر به تکه‌تکه شدن اینترنت شده است:

- روسیه برای مختل کردن زیرساخت‌های اوکراین با حملات سایبری، از زیرساخت‌های حیاتی مانند شبکه برق که منجر به قطع اینترنت می‌شود، استفاده کرده است.
- روسیه از طریق استفاده از تاکتیک‌های جنگ اطلاعاتی مانند تبلیغات و کمپین‌های اخبار جعلی به دنبال کنترل جریان اطلاعات در سراسر اوکراین است.
- روسیه به دنبال ایجاد یک اینترنت جداگانه و تحت کنترل خود، از طریق ابتکاراتی مانند توسعه روت‌سرورهای DNS و ایجاد یک «کلید قطع اینترنت»[۱] است.

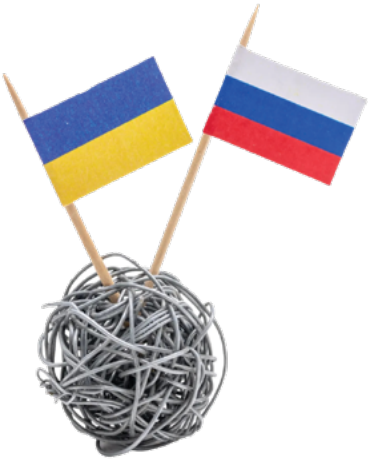
۱. kill switch، کلید قطع اینترنت، به توانایی یک دولت یا یک سازمان برای کنترل و متوقف کردن دسترسی به اینترنت در مقیاس گسترده اشاره دارد. این قابلیت منجر به این می‌شود که به طور موثر اتصال به اینترنت در یک منطقه، کشور یا شبکه‌های خاص، محدود یا قطع شود.

این گزارش پیامدهای این تکه‌تکه شدن اینترنت را به شرح ذیل برجسته می‌کند.

۱. تکه‌تکه شدن اینترنت جریان آزاد اطلاعات و توانایی افراد برای دسترسی به اطلاعات دقیق و قابل‌اعتماد را تضعیف می‌کند.
۲. تکه‌تکه شدن اینترنت پیامدهای ژئوپلیتیکی دارد، چراکه توانایی دولت‌ها برای مشارکت در دیپلماسی و مدیریت بحران را تضعیف می‌کند.
۳. تکه‌تکه شدن اینترنت منجر به ایجاد عواقب اقتصادی خواهد شد، زیرا زنجیره‌های عرضه جهانی را مختل نموده و توانایی شرکت‌ها برای فعالیت در خارج از مرزها را تضعیف می‌کند.
۴. تکه‌تکه شدن اینترنت تهدیدی برای ثبات و رفاه جهانی است.

به منظور مقابله و جلوگیری از فرایند تکه‌تکه شدن اینترنت، دولت‌ها و جامعه بین‌الملل موظف هستند مبادرت به اقدامات ذیل نمایند:

۱. افزایش سرمایه‌گذاری در امنیت سایبری و تاب‌آوری جهت محافظت از زیرساخت‌های حیاتی
۲. افزایش سرمایه‌گذاری در اقدامات دیپلماتیک و مدیریت بحران
۳. افزایش سرمایه‌گذاری در طرح‌هایی برای ترویج اینترنت آزاد و باز
۴. ارتقای سواد رسانه‌ای و مبارزه با اخبارجعلی



عنوان	Russia's War Against Ukraine is Catalyzing Internet Fragmentation
نویسنده	Christoph Meinel, David Hagebölling
مرکز مطالعاتی	CFR
تاریخ انتشار	March 13, 2023

انعطاف‌پذیری سایبری باید بر افراد به حاشیه رانده‌شده تمرکز کند!

این گزارش بنیاد کارنگی با تأکید بر ضرورت تغییر رویکرد نسبت به مفهوم انعطاف‌پذیری امنیت سایبری، اعلام می‌کند که توجه به نیازهای افراد و جوامع به حاشیه رانده‌شده (اقلیتی) که در برابر تهدیدات سایبری به‌طور خاصی آسیب‌پذیر هستند، نیازمند یک تغییر اساسی است. اگرچه، دولت‌ها وسازمان‌ها مدت‌هاست برای تأمین امنیت سایبری در تلاش بوده‌اند، اما تأثیر تهدیدات سایبری بر افراد به حاشیه رانده‌شده که اغلب فاقد منابع، دانش و دسترسی برای محافظت از خود هستند، مورد غفلت قرار گرفته است. در حالی که جوامع به حاشیه رانده‌شده اغلب در معرض بیشترین خطر هستند. این جوامع ممکن است فاقد منابع مالی برای سرمایه‌گذاری در اقدامات امنیتی سایبری قوی، دانش فنی برای محافظت از خود یا قدرت سیاسی برای دفاع از منافع خود باشند. مضافاً، این جوامع به حاشیه رانده‌شده (اقلیتی) ممکن است به‌طور نامتناسبی مورد هدف مجرمان سایبری باشند که به دنبال سوءاستفاده از آسیب‌پذیری‌های آن‌ها هستند.

رویکردهای فعلی نسبت به موضوع انعطاف‌پذیری امنیت سایبری بیشتر بر نهادها و زیرساخت‌های رسمی تمرکز دارند تا افراد و این چیزی است که باید تغییر کند. سیاست‌گذاران باید از یک رویکرد جامع‌تر که تأثیر تهدیدات سایبری را بر افراد و جوامع داده و برای رفع نیازهای آن‌ها گام بر می‌دارد، حمایت‌کنند. نویسنده برای حمایت از ایده خود از مطالعات موردی که آسیب‌پذیری جوامع به حاشیه رانده‌شده در مواجهه با تهدیدات سایبری را بررسی می‌کند، استفاده کرده است. او در مورد تأثیر جرائم سایبری بر افراد کم‌درآمد در آفریقای جنوبی، که بسیاری از مردم به خدمات بانکداری سنتی حتی دسترسی ندارند و بیشتر مورد هدف مجرمان سایبری قرار می‌گیرند، اشاره می‌کند و خطراتی که کارگران مهاجر در کشورهای خلیج‌فارس با آن روبرو بوده و ممکن است از طریق استفاده از تلفن همراه و رسانه‌های اجتماعی در معرض نظارت و استثمار قرار گیرند را بررسی می‌کند.

بر این اساس، اقداماتی که لازم است برای افزایش انعطاف‌پذیری امنیت سایبری جوامع به حاشیه رانده‌شده انجام گیرد، شرح ذیل است:

۱. سرمایه‌گذاری بیشتر در آموزش امنیت سایبری و برنامه‌های آگاهی‌بخش با هدف افراد و جوامع (اقلیتی)؛
۲. تمرکز تلاش‌های افزایش‌دهنده انعطاف‌پذیری امنیت سایبری بر رسیدگی به نابرابری‌های ساختاری؛
۳. سرمایه‌گذاری در تحقیق و توسعه جهت شناسایی تهدیدها و آسیب‌پذیری‌های جدید و توسعه فناوری‌ها و ابزارهای جدید برای کمک به افراد به حاشیه رانده‌شده جهت محافظت از خود.

عنوان	Cyber Resilience Must Focus On Marginalized Individuals, Not Just Institutions
نویسنده	Aubra Anthony
مرکز مطالعاتی	Carnegie
تاریخ انتشار	March 13, 2023

ساخت فرهنگ لغات مشترک برای استراتژی امنیت سایبری ملی

این گزارش با تأکید بر نیاز به توسعه فرهنگ لغت یا واژگان مشترک در استراتژی امنیت سایبری ملی، مطالعه‌ای جامع با تمرکز بر اهمیت درک مشترک مفاهیم و اصطلاحات امنیت سایبری بین سازمان‌های دولتی و بخش خصوصی پافشاری ارائه می‌دهد.

چالش‌های کلیدی در ایجاد فرهنگ لغت مشترک در استراتژی امنیت سایبری ملی عبارت‌اند از فقدان درک مشترک از مفاهیم کلیدی امنیت سایبری و استفاده از اصطلاحات مختلف توسط ذی‌نفعان. **فقدان فرهنگ لغت مشترک منجر به سردرگمی، عدم ارتباط، همکاری مؤثر و پیشرفت به سمت یک هدف مشترک می‌شود.**

برای رسیدگی به این چالش‌ها توصیه‌های زیر جهت توسعه واژگان مشترک برای استراتژی امنیت سایبری ملی به شرح ذیل پیشنهاد می‌شود.

- ایجاد یک **واژه‌نامه ملی امنیت سایبری** اکه اصطلاحات و مفاهیم کلیدی را به‌گونه‌ای سازگار و استاندارد تعریف کند. این واژه‌نامه باید از طریق یک فرایند مشترک که شامل همه ذی‌نفعان مربوطه، ازجمله سازمان‌های دولتی، انجمن‌های صنعتی و مؤسسات دانشگاهی است، توسعه یابد.
- ترویج استفاده از واژه‌نامه ملی امنیت سایبری از طریق برنامه‌های آموزشی و آگاهی‌بخشی به متخصصان دولت و صنعت. این امر به استفاده همه ذی‌نفعان از اصطلاحات و مفاهیم یکسان که موجب بهبود ارتباطات و همکاری خواهد شد، کمک می‌کند.
- ایجاد مکانیسمی جهت بررسی و به‌روزرسانی مداوم واژه‌نامه ملی امنیت سایبری به‌منظور اطمینان از مرتبط بودن و به‌روز بودن آن با تهدیدات و فناوری‌های نوظهور.

بخش ابتکار عمل سایبری شورای آتلانتیک بر اهمیت ایجاد درکی مشترک از مدیریت ریسک در استراتژی امنیت سایبری ملی تأکید دارد. از این رو، مدیریت ریسک باید کل‌نگر و با در نظر گرفتن کل اکوسیستم سایبری باشد و همه وابستگی‌های متقابل آن مورد توجه قرار گیرد. درک خطرات مرتبط با فناوری‌های نوظهور مانند هوش مصنوعی، محاسبات کوانتومی و اینترنت اشیا ازجمله این موارد است.

عنوان	Building a shared lexicon for the National Cybersecurity Strategy
نویسنده	the Cyber Statecraft Initiative
مرکز مطالعاتی	Atlanticcouncil
تاریخ انتشار	March 16, 2023

تحلیل فازی تاکتیکی عملیات آنلاین

گزارش «تحلیل فازی تاکتیکی عملیات آنلاین» بنیاد کارنگی، به تاکتیک‌های مورداستفاده توسط عوامل دولتی و غیردولتی در اجرای عملیات آنلاین می‌پردازد. عملیات آنلاین در طول زمان تکامل پیدا کرده و بازیگران اکنون از تاکتیک‌های پیچیده‌تری بهره می‌برند که تشخیص آن‌ها اغلب دشوار است. این گزارش چالش‌های کلیدی سیاست‌گذاران در این حوزه را شناسایی کرده و توصیه‌هایی برای رسیدگی به این چالش‌ها ارائه می‌کند.

عملیات آنلاین از چهار مرحله اصلی تشکیل می‌شود: **شناسایی، نفوذ، حمله و پس از حمله.** در مرحله شناسایی، عوامل مربوطه اطلاعاتی همچون آسیب‌پذیری‌ها و نقاط ضعف هدف را جمع‌آوری می‌کنند. در مرحله نفوذ، عوامل مربوطه به دنبال شکل دادن به ادراکات، نظرات و رفتارهای هدف از طریق اخبار جعلی، تبلیغات و سایر فن‌ها هستند. در مرحله حمله، عوامل مربوطه به دنبال اختلال، غیرفعال کردن یا به خطر انداختن شبکه‌ها، سیستم‌ها یا زیرساخت‌های هدف هستند؛ و در مرحله پس از حمله، عوامل مربوطه به دنبال حفظ دسترسی، استخراج داده‌ها یا پوشش مسیرهای خود هستند.

عملیات آنلاین با بهره‌برداری از طیف وسیعی از تاکتیک‌ها توسط عوامل دولتی، غیردولتی و نیروهای نیابتی انجام می‌گیرد. این تاکتیک‌ها شامل **مهندسی اجتماعی، فیشینگ، بدافزار، بات‌نت، حملات انکار سرویس توزیع‌شده (DDoS) و باج‌افزار** است. لازم به ذکر است که این تاکتیک‌ها در طول زمان پیچیده‌تر شده و بازیگران برای کمپین‌های اخبار جعلی متقاعدکننده‌تر از تکنیک‌های پیشرفته‌ای مانند **دیپ‌فیک** و **هوش مصنوعی** استفاده می‌کنند.

دولت‌ها در مقابله با عملیات آنلاین چالش‌های قابل‌توجهی مواجه هستند. یکی از این چالش‌ها دشواری انتساب است، زیرا بازیگران اغلب از تاکتیک‌هایی مانند جعل و سرورهای پروکسی برای پنهان کردن هویت واقعی خود استفاده می‌کنند. چالش دیگر سرعت بسیار بالای تغییرات فناورانه است که همگام شدن با تاکتیک‌ها و فن‌های جدید را برای دولت‌ها دشوار می‌کند. چالش دیگر فقدان هنجارها و توافقات بین‌المللی در خصوص استفاده از عملیات آنلاین است که هماهنگی پاسخ را برای دولت‌ها دشوار می‌کند.

در پاسخ‌به این چالش‌ها، دولت‌ها باید با انجام اقدامات زیر آسیب‌های ناشی از عملیات سایبری را کاهش داده و توانایی خود در مدیریت پیشینی و پسینی حملات را بهبود بخشند:

۱. تدوین مقررات و استانداردهای جدید برای صنعت فناوری جهت تشویق توسعه فناوری‌های ایمن‌تر و انعطاف‌پذیرتر؛
۲. بهبود هماهنگی بین‌المللی از طریق توسعه هنجارها و توافق‌نامه‌ها در خصوص استفاده از عملیات آنلاین؛
۳. بهبود قابلیت‌های انتساب حملات سایبری از طریق استفاده از پزشکی قانونی سایبری؛
۴. همکاری با بخش خصوصی و سرمایه‌گذاری در تحقیق و توسعه؛
۵. بهبود اشتراک‌گذاری اطلاعات تهدید بین کشورها و

سیاست‌گذاران نیازمند اتخاذ رویکردی جامع جهت پرداختن به عملیات آنلاین به‌جای تمرکز بر تاکتیک‌ها یا حوادث موردی هستند. چنین رویکردی باید شامل سرمایه‌گذاری در تحقیق و توسعه، همکاری با بخش خصوصی و تعاملات بین‌المللی باشد. سیاست‌گذاران باید برای ایجاد آگاهی عمومی و انعطاف‌پذیری در برابر عملیات آنلاین، به مردم در مورد خطرات آموزش داده و در مورد بهترین شیوه‌ها برای امنیت آنلاین راهنمایی ارائه کنند.

عنوان	Phase-based Tactical Analysis of Online Operations
نویسنده	Ben Nimmo, Eric Hutchins
مرکز مطالعاتی	Carnegie
تاریخ انتشار	March 16, 2023

درس‌های دفاع سایبری اوکراین برای تایوان

گزارش «درس‌های دفاع سایبری اوکراین برای تایوان» که توسط بنیاد دفاع از دموکراسی‌ها (FDD) منتشر شده، با مروری بر تجربه اوکراین در مقابله با تهدیدات سایبری، توصیه‌هایی را برای کشور تایوان ارائه و اهمیت برخورداری از یک استراتژی دفاع سایبری جامع شامل سرمایه‌گذاری در بخش فناوری، آموزش و همکاری با شرکای بین‌المللی را برجسته می‌کند.

در طول یک سال گذشته، اوکراین از سوی روسیه در معرض برخی از پیچیده‌ترین و طولانی‌ترین حملات سایبری قرار گرفته و ایالات‌متحده حمایت قابل‌توجهی از طریق کمک‌های فنی، کمک‌های مالی و به اشتراک‌گذاری اطلاعات از وی انجام داده است. تلاش برای خنثی‌سازی حملات به شبکه برق اوکراین، افزایش انعطاف‌پذیری حوزه انرژی، تربیت متخصصان امنیت سایبری و تسهیل اشتراک‌گذاری اطلاعات امنیت سایبری از اهم پشتیبانی‌های دولت بایدن از اوکراین است. FBI و فرماندهی سایبری ایالات‌متحده[۱] نیز نقش مهمی در شناسایی و مختل کردن فعالیت‌های سایبری مخرب روسیه ایفا کرده‌اند.

تایوان نیز که با تهدیدات سایبری همیشگی چین و خطر تصرف نظامی روبه‌رو است، می‌تواند از تجربه اوکراین در مقابله با حملات سایبری روسیه بیاموزد. با تکرار برنامه‌های موفق اوکراین، تایوان می‌تواند قابلیت‌های سایبری خود را افزایش دهد و خطر آسیب‌های زیرساختی ناشی از درگیری احتمالی با چین را کاهش دهد. با توجه به شرایط متشنج کنونی، این همکاری بین ایالات‌متحده و تایوان برای مقابله مؤثر با تهدیدات سایبری و حفاظت از منافع هر دو کشور ضروری است.

۱. U.S. Cyber Command

عنوان	Ukraine's Cyber Defense Offers Lessons for Taiwan
نویسنده	Lt Col James Hesson, Annie Fixler
مرکز مطالعاتی	FDD
تاریخ انتشار	March 16, 2023

اولویت سیاسی امنیت سایبری در آمریکای لاتین

شورای روابط خارجی در گزارشی درباره اولویت سیاسی امنیت سایبری در آمریکای لاتین به بررسی چالش‌هایی که کشورهای آمریکای لاتین در بهبود اقدامات امنیت سایبری خود با آن مواجه هستند پرداخته و گام‌هایی که سیاست‌گذاران در این کشورها می‌توانند برای مقابله با این چالش‌ها بردارند را تشریح می‌کند.

بر این اساس، عواملی که تاکنون منجر به اولویت پایین امنیت سایبری در این کشورها شده، عبارت است از **منابع محدود، چارچوب‌های نهادی ضعیف و عدم آگاهی عمومی.** این چالش‌ها با تهدیدات سایبری به‌سرعت در حال تغییر و فقدان تخصص فنی برای همگام شدن با این تغییرات در بسیاری از کشورهای آمریکای لاتین، تشدید می‌شوند. به منظور مقابله با این چالش‌ها، سیاست‌گذاران کشورهای آمریکای لاتین می‌بایست امنیت سایبری را در اولویت قرار داده و اقدامات ملموسی جهت بهبود وضعیت امنیت سایبری خود انجام دهند، ازجمله توسعه استراتژی‌های ملی امنیت سایبری، افزایش بودجه طرح‌های ملی امنیت سایبری و تقویت چارچوب‌های سازمانی و نهادی برای تقویت امنیت سایبری. علاوه بر این موارد، کشورهای آمریکای لاتین باید برای مقابله با چالش‌های مشترک امنیت سایبری با یکدیگر همکاری کنند. این همکاری به معنای اشتراک‌گذاری اطلاعات در مورد تهدیدات سایبری و همکاری در امر تحقیق و توسعه امنیت سایبری است و سازمان‌های منطقه‌ای مانند سازمان کشورهای آمریکایی می‌توانند در تسهیل این همکاری‌ها نقشی کلیدی ایفا کنند.

عنوان	Raising the Political Priority of Cybersecurity in Latin America
نویسنده	Louise Marie Hurel, Joe Devanny
مرکز مطالعاتی	CFR
تاریخ انتشار	March 16, 2023

واشنگتن مجدداً تلاش‌های ضد باج‌افزار را افزایش می‌دهد

این گزارش ضمن توصیف وضعیت فعلی تهدیدات باج‌افزار، افزایش شدید حملات در چند سال گذشته و نیز افزایش پیچیدگی‌های این تهاجمات، آخرین ابتکارات دولت ایالات‌متحده برای مبارزه با تهدیدات شدید حملات باج‌افزار را بررسی می‌کند. به‌تازگی، دولت آمریکا برای مقابله با این مشکل اقداماتی چون تشکیل گروه ویژه باج‌افزار و اخاذی دیجیتال و تشکیل یک گروه بین سازمانی جدید در اواخر سال ۲۰۲۲ برای هماهنگ کردن واکنش دولت به حملات باج‌افزارها انجام داده است.

در تازه‌ترین اقدام، آژانس امنیت سایبری و امنیت زیرساخت[1] (CISA) یک برنامه آزمایشی به نام آزمون هشدار آسیب‌پذیری باج‌افزار[2] (RVWP) راه‌اندازی کرده است تا به اپراتورهای تأمین‌کننده زیرساخت‌های حیاتی در شناسایی و رسیدگی به آسیب‌پذیری‌هایی که اغلب توسط بازیگران باج‌افزار مورد سوءاستفاده قرار می‌گیرند، کمک کند. این ابتکار نشان‌دهنده تعهد مداوم دولت بایدن برای مبارزه با حملات باج‌افزار به بخش خصوصی است. RVWPاز منابع و فناوری‌های موجود CISA برای شناسایی آسیب‌پذیری‌های امنیتی و مکان‌یابی دستگاه‌های متصل به اینترنت که مستعد حملات هستند، استفاده می‌کند.

۱. Cybersecurity and Infrastructure Security Agency
۲. Ransomware Vulnerability Warning Pilot

* * *

کارکنان CISA سپس از طریق ایمیل و تماس‌های تلفنی به شرکت‌های آسیب‌دیده اطلاع می‌دهند. در بررسی آزمایشی اولیه، ۹۳ سازمان از یک آسیب‌پذیری به نام «ProxyNotShell» در سرورهای Microsoft Exchange خود مطلع شدند و کارشناسان CISA توصیه‌هایی را در مورد چگونگی تعمیر سیستم‌های آسیب‌دیده ارائه کردند، زیرا بازیگران باج‌افزار، ازجمله گروه PlayCrypt، همچنان به هدف قرار دادن سیستم‌های اصلاح‌نشده ادامه می‌دهند. گروه PlayCrypt مسئول یک حمله باج افزار به Rackspace، یک شرکت محاسبات ابری مستقر در تگزاس، در ماه دسامبر بود که منجر به اختلال در خدمات ایمیل برای مشتریان متعدد شد.

به‌موازات اقدامات CISA، FBI و شرکای بین‌المللی نیز اقداماتی را برای مبارزه با باج‌افزار انجام داده‌اند. اخیراً، آن‌ها یک میکسر ارزهای دیجیتال [۱] را که توسط مجرمان سایبری برای پول‌شویی پرداخت‌های باج‌افزار و وجوه غیرقانونی استفاده می‌شد، غیرفعال کردند. وزارت دادگستری همچنین برخی از این افراد را دستگیر کرده و زیرساخت‌های دیجیتال آن‌ها را برای مختل کردن فرایند باج افزار مصادره کرده است.

این اقدامات همگی در راستای استراتژی امنیت سایبری دولت بایدن انجام شده که بر افزایش انعطاف‌پذیری زیرساخت‌های حیاتی در برابر باج افزارها و اقدامات مجریان قانون برای ایجاد اختلال در عملکرد بازیگران باج‌افزار تأکید دارد.

“

۱. cryptocurrency mixer، میکسر ارز دیجیتال همان‌طور که از نامش پیداست ابزاری برای ترکیب بیت‌کوین یا رمزارزهای دیگر با دارایی‌های دیجیتال یک کاربر تصادفی دیگر است. در این فرایند منبع دارایی‌ها پنهان شده و حریم شخصی کاربرانی که در معاملات دخیل هستند محافظت می‌شود. هنگامی که توکن‌های خود را با توکن‌های باقی کاربران ترکیب می‌کنید رهگیری عملیات مالی و دارایی‌های شما دشوار خواهد شد؛ میکسرها با ترکیب منابع مختلف با یکدیگر، شناسایی جزئیات تراکنشی را تقریباً غیرممکن خواهند ساخت.

عنوان	Washington Steps Up Anti-Ransomware Efforts, Again
نویسنده	Annie Fixler, Elysse Gregor
مرکز مطالعاتی	FDD
تاریخ انتشار	March 21, 2023

خطرات پیشنهاد جدید روسیه برای کنوانسیون سازمان ملل متحد در مورد امنیت اطلاعات بین‌المللی

شورای روابط خارجی (CFR) در یک گزارش تحلیلی، پیشنهاد روسیه برای کنوانسیون جدید سازمان ملل در خصوص امنیت اطلاعات بین‌المللی را بررسی و خطرات و عواقب آن را تحلیل کرده است. با توجه به پیامدهای منفی احتمالی چنین کنوانسیونی برای جامعه جهانی، شورای روابط خارجی از ایالات‌متحده و متحدانش می‌خواهد که از آن دوری کنند.

این گزارش ابتدا تاریخ روسیه در استفاده از مفهوم «امنیت اطلاعات» در توجیه اقدامات خود برای سرکوب آزادی بیان و محدود کردن دسترسی به اطلاعات را واکاوی می‌کند. دولت روسیه مدت‌ها است به دنبال رویکردی متمرکزتر در حکمرانی اینترنت بوده و سیستم فعلی توسط کشورهای غربی کنترل‌شده و علیه روسیه و سایر کشورهای غیر غربی سوگیری دارد. کنوانسیون پیشنهادی روسیه در مورد امنیت اطلاعات بخشی از تلاش برای تغییر شکل اینترنت مطابق با خواست و چشم‌انداز روسیه است. این کنوانسیون برای فضای سایبری قوانین جدیدی را وضع کرده که توانایی کشورها جهت انجام عملیات سایبری علیه یکدیگر را محدود و انتشار انواع خاصی از اطلاعات را ممنوع می‌کند. بااین‌حال، این قوانین در رژیم‌هایی مانند روسیه برای توجیه سانسور و سرکوب مخالفان سیاسی استفاده شده و پیشنهاد روسیه بخشی از یک گرایش گسترده به سمت کنترل هر چه بیشتر دولت بر اینترنت است. چین نیز در این زمینه پیشرو است و برای مسدود کردن دسترسی به وب سایت‌های خارجی و پلتفرم‌های رسانه‌های اجتماعی از فایروال بزرگ خود استفاده می‌کند. سایر کشورهای آسیایی هم از این روش پیروی کرده و ایران، عربستان سعودی و مصر همگی مدل‌های خود را اجرا می‌کنند.

بر این اساس، ایالات‌متحده و متحدانش باید در برابر پیشنهاد روسیه برای کنوانسیون سازمان ملل در خصوص امنیت اطلاعات بین‌المللی موضعی قوی اتخاذ کنند. برخی از اقداماتی که دولت ایالات‌متحده می‌تواند جهت مقابله با تلاش‌های روسیه انجام دهد عبارت است از:

۱. برشمردن پیامدهای منفی این کنوانسیون: دولت ایالات‌متحده باید مشخص کند این کنوانسیون توسط رژیم‌های مستبد و جهت سرکوب آزادی بیان و مخالفان سیاسی استفاده خواهد شد. ایالات‌متحده باید بر اهمیت حفظ اینترنت آزاد تأکید کند.

۲. همکاری با متحدان خود جهت مقابله با پیشنهاد روسیه: ایالات‌متحده باید برای عقب نشاندن پیشنهاد روسیه با متحدان خود همکاری کند. آمریکا و متحدانش باید از نهادهای چندجانبه مانند سازمان ملل برای ترویج آزادی اینترنت و مخالفت با هر تلاشی جهت محدود کردن دسترسی به اطلاعات استفاده کنند.

۳. سرمایه‌گذاری در دفاع سایبری: ایالات‌متحده و متحدانش باید برای دفاع در برابر حملات سایبری و سایر اشکال جنگ‌های اطلاعاتی در قابلیت‌های دفاع سایبری سرمایه‌گذاری کنند. این سرمایه‌گذاری شامل سرمایه‌گذاری در فناوری‌های جدید برای شناسایی و پاسخ به تهدیدات سایبری و بهبود انعطاف‌پذیری زیرساخت‌های حیاتی است.

۴. تعامل با جامعه مدنی: دولت آمریکا باید برای ترویج اینترنت آزاد و مخالفت با تلاش‌های سازمان‌یافته برای محدود کردن دسترسی به اطلاعات با جوامع مدنی و سایر ذی‌نفعان تعامل داشته و از گروه‌هایی که حامی اینترنت آزاد بوده و برای ارتقای سواد دیجیتال و سواد رسانه‌ای تلاش می‌کنند حمایت کند.

عنوان	The Dangers of a New Russian Proposal for a UN Convention on International Information Security
نویسنده	Valentin Weber
مرکز مطالعاتی	CFR
تاریخ انتشار	March 21, 2023

شبکه‌امنیت‌فضایی-سایبری‌هند

گزارش جدید ORFonline تحت عنوان «شبکه امنیت فضایی-سایبری هند» نیاز هند به ایجاد یک استراتژی جامع امنیت سایبری برای سرمایه‌های فضایی این کشور را بررسی کرده و تهدید رو به فزونی حملات سایبری علیه سیستم‌های فضایی و نیاز هند به اتخاذ اقدامات پیشگیرانه جهت محافظت از سرمایه‌های فضایی خود را برجسته می‌کند.

در طول سال‌های اخیر، اهمیت سرمایه‌های فضایی هند (همچون ماهواره‌ها و زیرساخت‌های پرتاب) برای امنیت ملی، رشد اقتصادی و تحقیقات علمی در این کشور به شدت افزایش یافته‌است، اما با استفاده بیشتر از این سرمایه‌های فضایی، خطر حملات سایبری به این سیستم‌ها نیز افزایش می‌یابد. هند باید برای مقابله با این تهدیدات و برای تضمین امنیت سرمایه‌های خود یک استراتژی جامع اتخاذ کند.

برخی حوزه‌های کلیدی که ضروری است در استراتژی امنیت فضایی-سایبری هند مورد توجه قرار گیرد، عبارت است از:

- **ادراک روشن و دقیق از تهدیدات پیش روی سرمایه‌های فضایی.** این ادراک به معنای شناسایی دشمنان سایبری بالقوه و روش‌های احتمالی حمله به سیستم‌های فضایی است. همچنین، هند باید یک چارچوب جامع مدیریت ریسک ایجاد کند که تأثیر بالقوه حملات سایبری بر دارایی‌های فضایی خود را در نظر گیرد.
- **توسعه زیرساخت‌های امنیت سایبری قوی برای محافظت از سرمایه‌های فضایی.** لازمه این زیرساخت‌ها اجرای کنترل‌های قوی دسترسی، رمزگذاری و احراز هویت برای جلوگیری از دسترسی غیرمجاز به سیستم‌های فضایی است. هند برای شناسایی و پاسخگویی فوری به تهدیدات سایبری، باید نظارت مستمری بر اطلاعات مربوط به تهدیدها انجام دهد.
- **همکاری‌های بین‌المللی در پرداختن به چالش‌های امنیت سایبری در سیستم‌های فضایی.** هند نیازمند آن است تا برای نیل به جایگاه برجسته جهانی، اقدام به اشتراک‌گذاری بهترین روش‌ها، اطلاعات تهدید و فناوری‌های امنیت سایبری با سایر کشورهای پیشرو فضایی کند و به شکل فزاینده‌ای برای توسعه هنجارها و استانداردهای رفتار مسئولانه در فضای سایبری در مجامع بین‌المللی مشارکت داشته باشد.

عنوان: India's space cybersecurity mesh: Criticality and call of purple revolution
نویسنده: Sudhansu Nayak
مرکز مطالعاتی: ORFonline
تاریخ انتشار: March 20, 2023

قانون‌گذاری و تنظیم‌گری

پرونده وزارت دادگستری علیه گوگل با کنگره همگام نیست

این گزارش پرونده اخیر ضدانحصار که توسط وزارت دادگستری ایالات‌متحده علیه گوگل تشکیل‌شده را مورد بررسی قرار می‌دهد. اینکه آیا اقدامات وزارت دادگستری آمریکا با دیدگاه‌های کنگره همسو هستند یا خیر؟ علی‌رغم آن‌که کنگره درباره قدرت بازار شرکت‌های فناوری بزرگ ازجمله گوگل ابراز نگرانی کرده است، به نظر می‌رسد که پرونده وزارت دادگستری علیه گوگل به‌جای نگرانی در خصوص موضوع ضدانحصار، بر موضوعات مرتبط با رتبه‌بندی موتورهای جستجو متمرکز است.

پرونده وزارت دادگستری علیه گوگل ادعا می‌کند که این شرکت برای حفظ سلطه خود در بازار موتورهای جستجو درگیر اقدامات ضدرقابتی است. وزارت دادگستری به‌طور خاص، ادعا می‌کند که گوگل از قدرت بازار خود برای تضمین قراردادهای انحصاری با سایر شرکت‌ها استفاده کرده و رقبا را در بازار به‌سختی می‌اندازد. با توجه به دیدگاه‌های کنگره در مورد موضوعات ضدانحصار در بخش فناوری، بسیاری از قانون‌گذاران در مورد قدرت بازار شرکت‌هایی مانند گوگل ابراز نگرانی کرده‌اند. با این حال، تمرکز کنگره بر روی موضوعات گسترده‌تر در حوزه رقابت، نوآوری و رفاه مصرف‌کننده بوده و صرفاً به موضوعات محدود مرتبط با رتبه‌بندی موتورهای جستجو محدود نشده است.

پرونده وزارت دادگستری علیه گوگل ممکن است با دیدگاه‌های کنگره مغایرت داشته باشد، زیرا به‌جای نگرانی در مورد رقابت و رفاه مصرف‌کننده، بر مسائل محدودی تمرکز دارد. این پرونده به قدرت بازار گوگل در بخش‌های دیگر، مانند تبلیغات آنلاین و پلتفرم‌های دیجیتال، نمی‌پردازد. این غفلت مخاطرات قابل ملاحظه‌ای در پی خواهد داشت، مانند احتمال آسیب رساندن به رقابت و نوآوری در بخش فناوری. در نتیجه باید توجه داشت که اگر اقدامات وزارت دادگستری علیه گوگل بیش‌ازحد تهاجمی یا با انگیزه سیاسی تلقی شود، می‌تواند تأثیری بدی بر دیگر شرکت‌های فناوری گذاشته و از نوآوری جلوگیری کند.

نویسنده توصیه می‌کند سیاست‌گذاران نسبت به موضوعات ضدانحصار در بخش فناوری رویکرد گسترده‌تری اتخاذ کرده و به‌جای موضوعات محدود در خصوص رتبه‌بندی موتورهای جستجو، بر ارتقای رقابت، نوآوری و رفاه مصرف‌کننده تمرکز کنند. با انجام این کار، سیاست‌گذاران یک اکوسیستم فناوری رقابتی را ترویج می‌کنند که به نفع مصرف‌کنندگان بوده و باعث رشد اقتصادی می‌شود.

عنوان: The Department of Justice's Case Against Google Seems out of Step with Congress
نویسنده: Mark Jamison
مرکز مطالعاتی: AEI
تاریخ انتشار: February 21, 2023

الگویی برای رویکرد مشارکتی نسبت به مقررات رقابت دیجیتال

این گزارش مدل جدیدی را برای مقررات رقابت دیجیتال ارائه می‌کند که بر اساس رویکردی نوآورانه بوده و طیف وسیعی از ذی‌نفعان را در فرایند سیاست‌گذاری درگیر می‌کند.

این گزارش چالش‌های پیش روی مقررات رقابت دیجیتال مانند سرعت سرسام‌آور نوآوری و دشواری در انطباق مقررات با فناوری‌های جدید را پررنگ کرده و خاطر نشان می‌کند، رویکرد نظارتی سنتی دیگر کافی نبوده و رویکرد مشارکتی‌تری برای رسیدگی به این چالش‌ها لازم است.

مدل پیشنهادی بر چهار اصل کلیدی استوار است: مشارکت چند ذی‌نفعی، تحلیل داده‌محور، توسعه سیاست‌های پیشین و حکمرانی انطباقی. هدف این اصول تضمین یک فرایند تنظیمی فراگیر، پاسخگو و قابل انطباق است.

این مدل می‌تواند از طریق ایجاد یک **مرکز ارزیابی رقابت دیجیتال** که به‌عنوان یک پلتفرم برای تعامل چند ذی‌نفعی و تجزیه‌وتحلیل داده‌محور عمل می‌کند، پیاده‌سازی شود. این مرکز مسئول ارزیابی جمع‌آوری داده‌ها در بازارهای دیجیتال، ارزیابی تأثیر فناوری‌های جدید، توسعه و اجرای سیاست‌های نظارتی خواهد بود.

این گزارش نقشه راه دقیقی برای اجرای مدل پیشنهادی نیز ارائه می‌دهد. این نقشه راه شامل ایجاد یک مرکز رصد و ارزیابی، توسعه چارچوب جامع جمع‌آوری و تجزیه‌وتحلیل داده‌ها، توسعه مجموعه‌ای از ابزارها و اقدامات سیاستی برای رسیدگی به مسائل مربوط به رقابت دیجیتال است.

سپس مزایای بالقوه این مدل، ازجمله افزایش شفافیت، افزایش مشارکت ذی‌نفعان و رویکرد مبتنی‌بر شواهد مورد بررسی قرار می‌گیرد. این مدل می‌تواند به رفع برخی از کاستی‌های فعلی مقررات رقابت دیجیتال، مانند فقدان چارچوب نظارتی جامع و دشواری در اجرای قوانین موجود نیز کمک کند.

بااین‌حال، نویسنده اذعان می‌کند که مدل پیشنهادی با چالش‌هایی مانند نیاز به هماهنگی زیاد بین ذی‌نفعان و پتانسیل جذب نظارتی مواجه است که این چالش‌ها نیز با طراحی و اجرای دقیق مدل برطرف می‌شود.

عنوان	A model for a participative approach to digital competition regulation
نویسنده	Christophe Carugati
مرکز مطالعاتی	Bruegel
تاریخ انتشار	February 27, 2023

بخش ۲۳۰ از غول‌های رسانه‌های اجتماعی محافظت می‌کند یا از مصرف‌کنندگان آمریکایی؟

این گزارش بنیاد هریتیج به موضوع چالشی و مهم بخش ۲۳۰ قانون شایستگی ارتباطات[۱] (CDA) و تأثیر آن بر مصرف‌کنندگان آمریکایی و پلتفرم‌های رسانه‌های اجتماعی می‌پردازد. بخش ۲۳۰ در سال ۱۹۹۶ و به‌منظور ترویج نوآوری و آزادی بیان در اینترنت در کنار محافظت از پلتفرم‌های اینترنتی در برابر مسئولیت محتوای ارسالی توسط اشخاص ثالث معرفی شد. بااین‌حال، شرکت‌های رسانه‌های اجتماعی از این حمایت قانونی برای سرکوب آزادی بیان و دست‌کاری گفتمان عمومی سوءاستفاده کرده‌اند که این امر منجر به بحث در مورد نیاز به اصلاح یا لغو آن شده است.

برخی کارشناسان استدلال می‌کنند که لغو یا اصلاح بخش ۲۳۰ به پلتفرم‌های رسانه‌های اجتماعی کوچک‌تر که نمی‌توانند از عهده رعایت مقررات سختگیرانه برآیند آسیب می‌زند و درنتیجه به نفع غول‌های بزرگ فناوری مانند فیس‌بوک و توییتر می‌شود. از سوی دیگر، طرفداران اصلاح بخش ۲۳۰ استدلال می‌کنند این موارد به شرکت‌های رسانه‌های اجتماعی امکان شرکت در سانسور انتخابی و تعدیل محتوا را داده و اصول آزادی بیان و گفتمان آزاد را نقض می‌کند.

۱. Communications Decency Act (CDA)

موضوع مهم در این میان آن نیست که بخش ۲۳۰ به طور کلی باید لغو یا اصلاح شود، بلکه باید مشخص شود که چگونه می‌توان آن را اصلاح کرد تا در خدمت منافع مصرف‌کنندگان آمریکایی باشد. بر همین اساس، می‌توان از رویکردی هدفمندتر برای تعدیل محتوا و حفاظت از مسئولیت برای شرکت‌های رسانه‌های اجتماعی، به‌جای استفاده از یک رویکرد یکسان برای همه، استفاده کرد.

به پیشنهاد این گزارش کنگره باید استاندارد «حسن نیت» را در پیش گرفته و ضمن محافظت از پلتفرم‌های رسانه‌های اجتماعی که با حسن نیت برای حذف محتوای غیرقانونی عمل می‌کنند، آن‌ها را برای حذف عمدی یا بی‌ملاحظگی در محتوا، مسئول نداند. در مقابل، شرکت‌های رسانه‌های اجتماعی باید در شیوه‌های تعدیل محتوای خود شفاف‌تر باشند و به مصرف‌کنندگان اجازه دهند تا درخواست بررسی حذف محتوا بدهند.

نقش قوانین رقابت و ضدانحصار در پرداختن به مسائل مربوط به بخش ۲۳۰ نیز موضوع مهم دیگری است که مورد بررسی قرار می‌گیرد. رقابت می‌تواند ابزار مؤثری برای رسیدگی به مشکل تعدیل محتوا باشد و اعمال قوانین ضدانحصار برای جلوگیری از اقدامات ضد رقابتی شرکت‌های رسانه‌های اجتماعی ضروری است.

بر همین اساس، باید توجه داشت که بخش ۲۳۰ یک موضوع کم اهمیت نیست، بلکه پیامدهایی برای سیاست خارجی و امنیت ملی ایالات‌متحده در پی دارد و دولت آمریکا باید از قدرت دیپلماتیک و اقتصادی خود برای متقاعد کردن دولت‌های خارجی برای اتخاذ سیاست‌هایی که از آزادی بیان محافظت و از سانسور آنلاین جلوگیری می‌کند، استفاده کند.

عنوان	?Does Section 230 Protect Big Social Media or American Consumers
نویسنده	Theodore Wold
مرکز مطالعاتی	Heritage
تاریخ انتشار	February 21, 2023

مقابله با تروریسم خشن با انگیزه‌های نژادی و قومیتی در شبکه‌های اجتماعی

در سال‌های اخیر، در پاسخ به حملات خشن افراطگرایان با انگیزه‌های نژادی و قومیتی [۱] (REMVE)، به فضاهای آنلاین که در آن این افراطگریان با دیگران هماهنگ شده و دیدگاه‌های خود را منتشر می‌کنند، توجه بیشتری شده است. اما درک بحث‌ها، عبارات و زبان استفاده شده در این محیط‌های آنلاین می‌تواند برای کسانی که خارج از این محیط‌ها هستند چالش‌برانگیز باشد. چراکه زبان مورداستفاده می‌تواند عمداً مبهم باشد، سریعاً تکامل یابد، مکرراً رخ دهد و تجزیه‌وتحلیل دستی متن آنلاین را غیرممکن کند. پژوهشگران اندیشکده RAND جهت تسهیل تحلیل این فضاها، روشی ایجاد کرده و ابزاری به نام RVE-Flock را برای شناسایی و درک اصطلاحات نوظهور توسعه داده‌اند که تحلیل و تکامل آن‌ها را در بخش واژگان آنلاین وب‌سایت‌های خاصی ممکن می‌کند.

این ابزار می‌تواند با استفاده از پردازش زبان طبیعی، میزان ظهور اصطلاحات مختلف را بر اساس معیارهای گوناگونی چون افزایش در استفاده، تغییرات در زمینه، یا افزایش در انجمن‌ها یا وب‌سایت‌های دیگر شناسایی کند. این تجزیه‌وتحلیل از پردازش زبان طبیعی بهره می‌گیرد تا میزان ظهور اصطلاحات مختلف را بر اساس معیارهای گوناگونی چون افزایش در استفاده، تغییرات در زمینه آن‌ها یا تکثیر در انجمن‌ها یا وب‌سایت‌های دیگر تعیین کند. در این تحلیل، پژوهشگران این معیارها را بر روی پست‌های ارسال‌شده در (/pol/ ۴chan) اعمال کرده تا پتانسیل این ابزار را در شناسایی اصطلاحات نوظهور و تسهیل کاوش و تعریف این اصطلاحات نشان دهند.

۱. Racially and ethnically motivated violent extremist (REMVE)

آن‌ها در این گزارش برای نمایش توانایی این ابزار در زمینه‌سازی اصطلاحات و ردیابی تکامل آن‌ها در طول زمان بر مجموعه‌ای از اصطلاحات خیلی خاص و نامتعارف، مثل اصطلاحات (glowies and glown----r)[1] تمرکز می‌کنند (بخش دوم این اصطلاح یک توهین نژادی است).

نتایج به دست آمده در پایان این مطالعه اثبات می‌کند که ابزار توسعه‌یافته، ابزاری قدرتمند برای شناسایی اصطلاحات نوظهور در محیط‌های آنلاینی است که حملات خشن افراط‌گرایان با انگیزه‌های نژادی و قومیتی در آن اتفاق می‌افتد و کاوش و تعریف استفاده از اصطلاحات را برای افرادی که با این محیط‌ها بیگانه هستند، تسهیل می‌کند. از سوی دیگر، با استفاده از معیارهای این ابزار برای تشخیص چگونگی تکامل اصطلاحات نوظهور، می‌توان ایدئولوژی‌ها و تاکتیک‌های افراط‌گرایان خشن را بهتر درک کرده و برای جلوگیری از اقدامات مضر آن‌ها اقدام کرد.

۱. اصطلاح فوق اصطلاحی است که توسط افراد افراطی مخصوصا بعد از شورش‌های ۶ ژانویه ۲۰۲۱ به کار برده می‌شود. افراط گرایان ظاهراً از دستگیری هراسی ندارند، اما از Glowies می‌ترسند. در دوران دولت ترامپ، دغدغه اصلی بسیاری از گروه‌های راست افراطی این بود که چگونه افراد بیشتری را به این هدف جذب کنند. در همین حال مقامات مجری قانون فدرال به دستگیری افراد مظنون به دست داشتن در قیام ۶ ژانویه ادامه دادند و جو بایدن وعده سرکوب افراط‌گرایان

عنوان: Countering Domestic Racially and Ethnically Motivated Violent Terrorism on Social Media
نویسنده: Daniel Tapia, Kristin Warre, Jacqueline Gardner Burns, Khrystyna Holynsk, Jordan R. Reimer, Peter Schirme, Will Shumate
مرکز مطالعاتی: Rand
تاریخ انتشار: February 23, 2023

تنظیم‌گری پلتفرم‌های دیجیتال: حکمرانی بر چیزی که غیرقابل کنترل است.

ظهور پلتفرم‌های دیجیتال به یک معمای نظارتی تبدیل شده است، معمایی که دولت‌ها باید بدون نابود کردن نوآوری به تنظیم این پلتفرم‌ها مبادرت کنند. چاتم هاوس در این گزارش، به تحلیل چالش‌های تنظیم پلتفرم‌های دیجیتال پرداخته و توصیه‌هایی را برای نحوه حکمرانی دولت‌ها بر مسائل غیرقابل حکمرانی ارائه می‌دهد.

این گزارش با بحث در مورد چالش‌های تنظیم پلتفرم‌های دیجیتال، مثل ماهیت فراملی این پلتفرم‌ها، سرعت نوآوری و پویایی قدرت بین پلتفرم‌ها و کاربران آن‌ها آغاز می‌شود. با اینکه خودتنظیمی کافی نبوده، با توجه به ماهیت سریع و در حال تغییر پلتفرم‌ها رویکردهای نظارتی سنتی نیز همیشه ممکن یا مؤثر نیستند. رویکرد جدیدی که باید مورد توجه قرار گیرد، شامل تلفیقی از اشکال جدید خودتنظیمی، تنظیم‌گری مشترک با دولت و مداخله مستقیم دولت است. این رویکردها می‌توانند به ایجاد تعادل در نیاز به نظارت کمک کنند و درعین‌حال نوآوری و رقابت را میسر نمایند.

خودتنظیمی باید بر اساس شفافیت، پاسخگویی و توانمندسازی کاربران پایه‌گذاری شود. این عمل می‌تواند شامل اقداماتی مانند شرایط خدمات روشن و در دسترس، تنظیمات حریم خصوصی داده‌های کاربر و سیاست‌های شفاف نظارت بر محتوا باشد. **یک نظام مقرراتی مشارکت‌محور که در آن صنعت و دولت با هم کار می‌کنند، می‌تواند به پر کردن شکاف‌های نظارتی و اطمینان از رعایت استانداردها کمک کند. ایجاد استانداردهای رفتار صنعتی یا ایجاد نهادهای نظارتی مستقل نمونه‌ای برای این امر است.**

از سوی دیگر، مداخله مستقیم دولت باید هدفمند و متناسب باشد. این مداخله می‌تواند شامل اقداماتی مانند گزارش اجباری محتوای مضر یا الزامات شفافیت الگوریتمی باشد، اما مداخله دولت باید بااحتیاط انجام شود، زیرا مقررات بیش‌ازحد و تورم تقنینی می‌تواند نوآوری را نابود و به رقابت آسیب برساند.

اهمیت همکاری بین‌المللی در تنظیم سیستم عامل‌های دیجیتال به دلیل ماهیت فراملیتی آن‌ها مسئله مهم دیگری است که باید مورد توجه قرار گیرد. توافق‌نامه‌ها و استانداردهای بین‌المللی می‌توانند به تضمین محیط برابر و کاهش پراکندگی مقررات کمک کنند.

این گزارش با توصیه‌هایی در خصوص چگونگی برقراری تعادل بین نظارت با نوآوری و رقابت توسط سیاست‌گذاران به پایان می‌رسد. نویسندگان پیشنهاد می‌کنند که تنظیم‌کننده‌ها باید به‌جای واکنش‌های پسینی، رویکردی فعالانه و پیشینی داشته، مسائل نوظهور را پیش‌بینی و به آن‌ها رسیدگی کنند. همچنین نیاز به گفت‌وگوی مداوم بین صنعت، دولت و جامعه مدنی منجر به اطمینان خاطر از این امر مهم خواهد شد که رویکردهای نظارتی مؤثر و پایدار هستند.

عنوان	Digital platform regulation: Governing the ungovernable
نویسنده	Yasmin Afina
مرکز مطالعاتی	Chathamhouse
تاریخ انتشار	February 24, 2023

واشنگتن در مورد چین و استانداردهای فنی چه اشتباهی می‌کند؟

این گزارش به دنبال ارائه دیدگاهی جایگزین در مورد رویکرد چین به تنظیم استاندارد در فناوری است و خطرات رویکرد کنونی ایالات‌متحده را بررسی می‌کند. **استراتژی کنونی واشنگتن برای محدودکردن مشارکت چین در تلاش‌های تعیین استاندارد جهانی، غلط است و نتیجه معکوس در پی خواهد داشت، زیرا این خطر عزم چین برای توسعه استانداردهای خود و تبدیل شدن به یک ابرقدرت فناوری را بیشتر می‌کند.** با توجه به این نکته مهم، به نظر می‌رسد که رویکرد مشارکتی‌تری نیاز است که در آن ایالات‌متحده با چین تعامل کند تا استانداردها و مقررات فنی جهانی را به‌گونه‌ای شکل دهد که از منافع هر دو کشور محافظت نموده و نوآوری و رقابت را بیفزاید.

نویسندگان یک نمای کلی از وضعیت فعلی تنظیم استانداردهای فنی جهانی ارائه می‌کند و بر اهمیت روزافزون این استانداردها در طیف وسیعی از زمینه‌ها، از مخابرات و حکمرانی اینترنت گرفته تا وسایل نقلیه خودران و هوش مصنوعی تأکید می‌کند. چین در سال‌های اخیر شدیداً در این زمینه‌ها فعال بوده و به دنبال ایجاد استانداردهای خود و ایفای نقش بیشتری در توسعه استانداردهای جهانی است. **این تغییر تا حدی ناشی از تمایل چین برای تضمین حکمرانی فناورانه خود و کاهش اتکای این کشور به فناوری‌های خارجی است و بیانگر گرایش عمومی به سمت جهانی چندقطبی‌تر است که در آن قدرت‌های نوظهور به دنبال نمایندگی و نفوذ بیشتر در ساختارهای حکمرانی جهانی آن هستند.**

سپس به وضعیت کنونی روابط ایالات‌متحده و چین پرداخته شده و رویکردی را که ایالات‌متحده از طریق آن به دنبال محدود کردن مشارکت چین در تلاش‌های جهانی برای تنظیم استانداردها است، بررسی می‌شود. این رویکرد مبتنی‌بر یک فرض اساسی و ناقص است: این‌که چین در درجه اول به تسلط بر استانداردهای جهانی علاقه‌مند است تا رهبری فناورانه ایالات‌متحده را تضعیف و قدرت ژئوپلیتیکی خود را تقویت کند. اگرچه ممکن است بخشی از این دیدگاه حقیقت داشته باشد، اما انگیزه‌های چین بیش‌ازحد ساده گرفته شده و این واقعیت را که چین نگرانی‌های درستی در مورد خطرات قفل شدن استانداردها و مقررات کلیدی فناوری دارد نادیده می‌گیرد.

بر همین اساس، اتخاذ رویکردی مشارکتی‌تر برای تنظیم استانداردهای جهانی ضروری است، رویکردی که هم ایالات‌متحده و چین و هم سایر ذی‌نفعان را در فرایندی مشترک برای شکل‌دهی استانداردها و مقرراتی که رقابت، نوآوری و احترام را ترویج می‌کند، درگیر کند. حریم خصوصی و حقوق بشر در چنین رویکردی نیازمند سرمایه‌گذاری زیادی در تخصص فنی و ظرفیت دیپلماتیک و تمایل به تعامل با چین در مورد موضوعات دوجانبه است. همچنین باید دانست استانداردهای فنی صرفاً مسائلی فنی نیستند، بلکه در بطن خود عمیقاً سیاسی و استراتژیک بوده و منافع و ارزش‌های رقیب را منعکس می‌کنند.

این گزارش با مجموعه‌ای از توصیه‌ها در مورد چگونگی سوق یافتن ایالات‌متحده به سمت رویکرد مشارکتی‌تر برای تنظیم استانداردهای جهانی به پایان می‌رسد. این امر شامل سرمایه‌گذاری در تخصص فنی و ظرفیت دیپلماتیک، تعامل با چین به شیوه‌ای سازنده و مشارکتی و تلاش برای ارتقای شفافیت و فراگیری در تلاش‌های تنظیم استانداردهای جهانی است.

عنوان	What Washington Gets Wrong About China and Technical Standards
نویسنده	Matt Sheehan, Jacob Feldgoise
مرکز مطالعاتی	Carnegie
تاریخ انتشار	February 27, 2023

کنگره برای تصویب قانون حفظ حریم خصوصی داده‌ها نیاز به درک نحوه عملکرد تبلیغات آنلاین دارد

این گزارش به ضرورت درک چگونگی کارکرد تبلیغات آنلاین برای توسعه قوانین مناسب در حفظ حریم خصوصی داده‌ها و چالش‌های قوانین حفظ حریم خصوصی داده‌ها در ایالات‌متحده را مورد بررسی قرار می‌دهد. این گزارش در ادامه برخی اصول کلیدی برای قانون حفظ حریم خصوصی داده‌ها را برمی‌شمارد که می‌تواند بین نیاز به نوآوری و نیاز به حفظ حریم خصوصی مصرف‌کننده تعادل برقرار کند.

لزوم شناخت بازیگران تبلیغات آنلاین

بازیگران مختلف درگیر در فرایند تبلیغات مانند تبلیغ‌کنندگان، ناشران، مبادله‌گران تبلیغات و کارگزاران داده هستند که از طریق روش‌های جمع‌آوری و استفاده از داده‌های مصرف‌کننده، چرخه تبلیغات را به حرکت در می‌آورند. ضروری است تا سیاست‌گذاران با شناخت دقیق این بازیگران و فرایند عملکرد قوانین متناسبی به منظور حفاظت از حریم خصوصی داده‌ها تصویب کنند.

لزوم شفافیت و پاسخگویی در صنعت تبلیغات آنلاین

سیاست‌گذاران باید دستورالعمل‌های مشخصی را برای جمع‌آوری، استفاده و اشتراک‌گذاری داده‌های مصرف‌کننده در تبلیغات آنلاین ایجاد کنند. اقدامات شفاف‌سازی و مسئولیت‌پذیری، مانند رضایت انتخاب و امکان دسترسی و کنترل مصرف‌کنندگان در داده‌هایشان، از اهم این اقدامات است.

لزوم برقراری تعادل بین نوآوری و حریم خصوصی

سیاست‌گذاران باید مزایای بالقوه تبلیغات آنلاین، همچون حمایت از کسب‌وکارهای کوچک و محتوای رایگان در اینترنت را در نظر بگیرند و به تهدیدات حریم خصوصی آن نیز توجه کنند. قانون حفاظت از حریم خصوصی داده‌ها باید اطلاعات حساس مانند داده‌های بهداشتی و مالی را در اولویت قرار دهد و امکان جمع‌آوری و استفاده از داده‌های غیرحساس برای اهداف تبلیغاتی را فراهم نکند.

لزوم درک اکوسیستم تبلیغات آنلاین

سیاست‌گذاران باید ضمن توجه به اقتضائات صنعت تبلیغات آنلاین، اقدام به وضع قوانین مناسب در خصوص حفظ حریم خصوصی داده‌ها کرده و با صنعت و جامعه مدنی برای اتخاذ بهترین روش‌ها در حفظ حریم خصوصی داده‌ها و شفافیت در تبلیغات آنلاین همکاری کنند. سیاست‌گذاران باید با در نظر گرفتن خطرات گوناگون حریم خصوصی داده‌ها در بخش‌ها و صنایع مختلف، رویکردی جامع نسبت به قانون حفظ حریم خصوصی داده‌ها داشته باشند.

عنوان	Congress Needs to Understand How Online Ads Work to Pass Data Privacy Legislation
نویسنده	Daniel Castro
مرکز مطالعاتی	ITIF
تاریخ انتشار	March 2, 2023

قوانین طلایی برای تنظیم کالاهای عمومی دیجیتال

این گزارش بر نیاز به چارچوب‌های نظارتی جهت حمایت از ایجاد و انتشار کالاهای عمومی دیجیتال تأکید داشته و اهمیت کالاهای عمومی دیجیتال در دستیابی به اهداف توسعه پایدار و نیاز به محیطی مناسب برای توسعه و استقرار آن‌ها را ضروری می‌داند. سه «قانون طلایی» برای تنظیم کالاهای عمومی دیجیتال عبارتند از:

۱. اولویت قراردادن حریم خصوصی و امنیت کاربر؛
۲. اطمینان از قابلیت همکاری؛
۳. ارتقای باز بودن و شفافیت.

قانون اول نیاز به محافظت از داده‌های کاربر و اطمینان از طراحی کالاهای عمومی دیجیتال با در نظر گرفتن حریم خصوصی و امنیت افراد را عنوان می‌کند. قانون دوم اطمینان از اینکه کالاهای عمومی دیجیتال می‌توانند یکپارچه و بدون ممانعت با هم کار کنند را برجسته می‌کند و قانون سوم، اهمیت شفافیت و باز بودن در توسعه و استقرار کالاهای عمومی دیجیتال را بیان می‌کند. این سه قانون برای ایجاد یک چارچوب نظارتی که از توسعه کالاهای عمومی دیجیتال پشتیبانی نماید ضروری است. این گزارش به ارائه نمونه‌هایی از کالاهای عمومی دیجیتال مثل نرم‌افزارهای متن‌باز پرداخته و تأثیر آن‌ها بر دستیابی به اهداف توسعه پایدار را نشان می‌دهد. کالاهای عمومی دیجیتال را می‌توان از طریق ذی‌نفعان مختلفی مانند دولت‌ها، سازمان‌های غیرانتفاعی و بخش خصوصی ایجاد و نگهداری کرد.

از سوی دیگر، توجه به چالش‌های تنظیم‌گری نیز ضروری به نظر می‌رسد و بر همین اساس، توصیه‌هایی برای سیاست‌گذاران در این خصوص مطرح می‌شود. یکی از توصیه‌ها اتخاذ یک رویکرد چندجانبه در حکمرانی کالاهای عمومی دیجیتال است که شامل همکاری بین دولت‌ها، سازمان‌های غیرانتفاعی و بخش خصوصی است. سیاست‌گذاران می‌بایست هنگام تنظیم کالاهای عمومی دیجیتال، حریم خصوصی و امنیت کاربران را در اولویت قرار داده و از قابلیت همکاری و باز بودن آن‌ها اطمینان حاصل کنند. اهمیت کالاهای عمومی دیجیتال در دستیابی به اهداف توسعه پایدار و نیاز به یک چارچوب نظارتی که از توسعه و استقرار آن‌ها حمایت می‌کند، از دیگر نکات مهمی است که مورد بررسی قرار می‌گیرند. کالاهای عمومی دیجیتال می‌توانند به ساختن جهانی فراگیرتر، عادلانه‌تر و پایدارتر کمک نموده و تنظیم مؤثر این کالاها برای تحقق کامل ارتباطات و اطلاعات ملی ضروری است.

عنوان	Golden rules for regulating Digital Public Goods
نویسنده	Johanna Weaver
مرکز مطالعاتی	ORFonline
تاریخ انتشار	March 3, 2023

نظراتی در باب اداره ملی مخابرات و ارتباطات درباره حریم خصوصی، برابری و حقوق مدنی

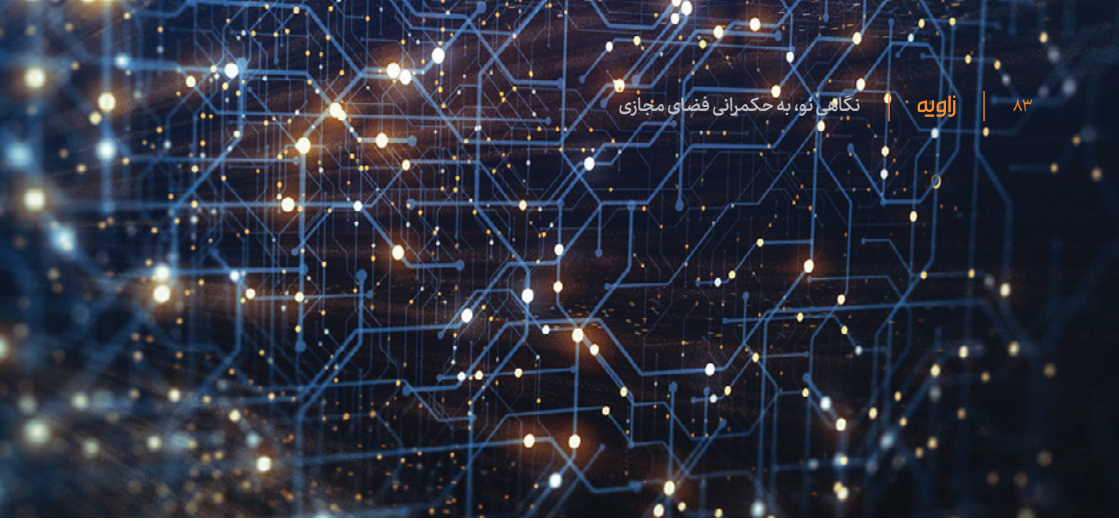
این گزارش در مورد توسعه چارچوب حریم خصوصی، برابری و حقوق مدنی جهت استفاده از فناوری‌های نوظهور بازخوردی به اداره ملی مخابرات و اطلاعات می‌دهد. نویسنده نیاز به اتخاذ یک رویکرد متعادل در حفاظت از حریم خصوصی و برابری به‌گونه‌ای که مزایا و مضرات بالقوه فناوری‌های نوظهور را در نظر گیرد، برجسته می‌کند.

فناوری‌های نوظهور مثل هوش مصنوعی مزایای بالقوه زیادی داشته و در بهبود مراقبت‌های بهداشتی، آموزشی و سایر موارد اجتماعی توانایی‌های قابل توجهی دارند؛ اما خطرات بالقوه ناشی از استفاده از این فناوری‌ها، همچون تعصب الگوریتمی و تبعیض را نیز نباید نادیده گرفت. بر همین اساس، ضروری است تا یک رویکرد متوازن اتخاذ گردد که هم مزایا و هم خطرات بالقوه فناوری‌های نوظهور در افزایش حریم خصوصی، برابری و حقوق مدنی را در نظر بگیرد. اهمیت اطمینان از اینکه حفاظت از حریم خصوصی مانع نوآوری نمی‌شود در همین رهگذر نمایان می‌شود. در نتیجه، اداره ملی مخابرات و اطلاعات باید به‌جای قوانین سفت‌وسخت، بر توسعه چارچوب‌های حریم خصوصی که انعطاف‌پذیر و سازگار با فناوری‌های نوظهور هستند تمرکز کرده و با صنعت، جامعه مدنی و دیگر ذی‌نفعان در توسعه چارچوب‌های حفظ حریم خصوصی که مروج نوآوری هستند و از حریم خصوصی و حقوق مدنی محافظت می‌کنند، همکاری کند.

اهمیت ارتقای برابری و فراگیری در توسعه و استفاده از فناوری‌های نوظهور نیز مسئله مهمی است که باید به آن توجه کرد. اداره ملی مخابرات و اطلاعات، توسعه و استفاده از فناوری‌های نوظهور را باید به نحوی اولویت دهد تا به نفع همه اعضای جامعه، ازجمله جوامع حاشیه‌ای باشد. این اداره باید برای درک نیازها و نگرانی‌های آن‌ها و توسعه سیاست‌ها و چارچوب‌هایی که برابری و فراگیری را ارتقا می‌دهد، با این جوامع همکاری کند.

نیاز به شفافیت و پاسخگویی در توسعه و استفاده از فناوری‌های نوظهور نیز از دیگر موضوعاتی است که اداره ملی مخابرات و اطلاعات باید از طریق وضع دستورالعمل‌های مشخصی در خصوص جمع‌آوری، استفاده و اشتراک‌گذاری داده‌ها مورد توجه قرار دهد. این مسئله در زمان توسعه فناوری‌های نوظهور و مکانیسم‌هایی مانند بازرسی و الزامات گزارش برای پاسخگویی موضوعیت پیدا می‌کند تا از حفظ حریم خصوصی و آزادی‌های مدنی در توسعه و استفاده از فناوری‌های نوظهور اطمینان حاصل شود.

عنوان	Comments to the NTIA Regarding Privacy, Equity, and Civil Rights
نویسنده	Ashley Johnson
مرکز مطالعاتی	ITIF
تاریخ انتشار	March 6, 2023



برقراری تعادل در حفاظت از حریم خصوصی و نوآوری در شهرها و جوامع هوشمند

این گزارش چالش‌ها و فرصت‌های پیاده‌سازی فناوری‌های شهر هوشمند را ضمن حفاظت از حریم خصوصی و امنیت داده‌های شخصی شهروندان تحلیل و بررسی می‌کند. فناوری‌های شهر هوشمند مزایای بالقوه‌ای مانند بهبود کارایی، کاهش هزینه‌ها و افزایش کیفیت زندگی دارند و موازات توجه به این مزایا، باید به خطرات مربوط به حریم خصوصی و امنیتی ناشی از جمع‌آوری، ذخیره‌سازی و استفاده از داده‌های شخصی شهروندان نیز توجه داشت. بر همین اساس، سیاست‌گذاران، صنعت و جامعه مدنی جهت رسیدگی به این نگرانی‌ها نیازمند دستورالعمل‌هایی هستند تا از برقراری تعادل بین حریم خصوصی و نوآوری در توسعه شهرهای هوشمند اطمینان حاصل کنند.

نیاز به یک چارچوب جامع در خصوص حریم خصوصی و امنیت برای فناوری‌های شهر هوشمند

سیاست‌گذاران باید دستورالعمل‌های مشخصی برای جمع‌آوری، استفاده و ذخیره‌سازی داده‌های شخصی ایجاد و برای تضمین شفافیت و پاسخگویی مکانیسم‌هایی اتخاذ کنند. صنعت و جامعه مدنی نیز باید در توسعه بهترین شیوه‌ها جهت حفاظت از داده‌ها و امنیت سایبری ایفای نقش کنند.

لزوم مشارکت و همکاری شهروندان در توسعه شهرهای هوشمند

سیاست‌گذاران و صنعت باید شهروندان را در فرایند تصمیم‌گیری مشارکت دهند و جویای نظرات آن‌ها در مورد فناوری‌های شهر هوشمند باشند. مشارکت شهروندان می‌تواند به ایجاد اعتماد و اطمینان در فناوری‌های شهر هوشمند کمک کند و از همسویی این فناوری‌ها با نیازها و ارزش‌های شهروندان اطمینان حاصل نماید.

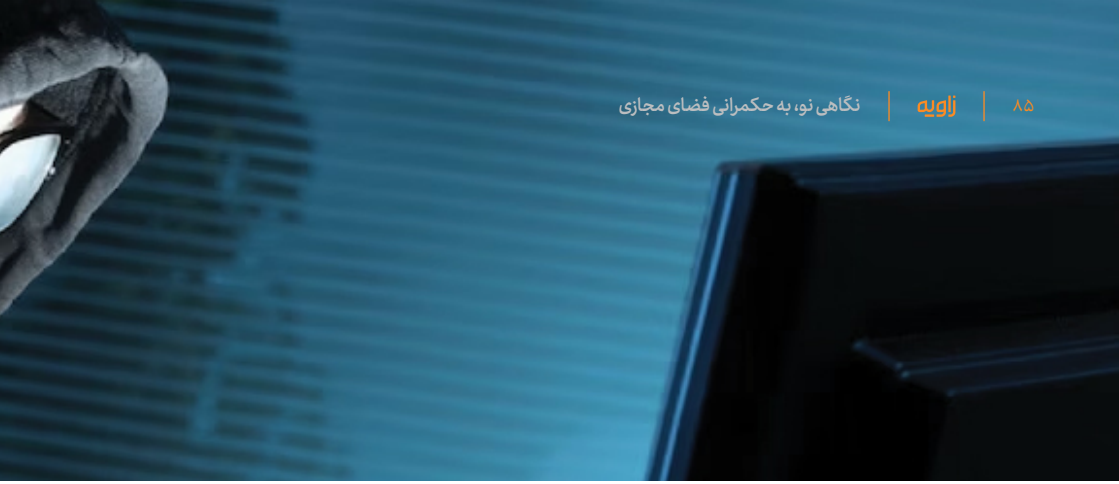
اهمیت حکمرانی داده و اشتراک‌گذاری داده در توسعه شهر هوشمند

سیاست‌گذاران و صنعت باید برای به اشتراک‌گذاری و استفاده از داده‌ها قوانین و استانداردهای مشخصی را ایجاد کنند تا از کنترل شهروندان بر داده‌های شخصی‌شان اطمینان حاصل شود. چارچوب‌های حکمرانی داده باید بین نیاز به دسترسی به داده‌ها و نوآوری و نیاز به حفظ حریم خصوصی و امنیت تعادل برقرار کنند.

جایگاه نوآوری در توسعه شهر هوشمند

سیاست‌گذاران و صنعت باید توسعه فناوری‌های نوآورانه‌ای را در اولویت بگذارند که کارایی و اثربخشی خدمات شهر هوشمند را بهبود می‌بخشد و در عین حال، از حفظ حریم خصوصی و امنیت شهروندان نیز اطمینان حاصل می‌کند. نوآوری باید بر اساس مجموعه‌ای از اصول و ارزش‌های اخلاقی مدیریت شود تا منافع عمومی و رفاه شهروندان را در اولویت قرار دهد.

عنوان	Balancing Privacy and Innovation in Smart Cities and Communities
نویسنده	Ashley Johnson
مرکز مطالعاتی	ITIF
تاریخ انتشار	March 6, 2023



مقررات استفاده دوگانه: مدیریت نفرت و تروریسم آنلاین قبل و بعد از اصلاح بخش ۲۳۰

این گزارش اندیشکده بروکینگز، چالش‌های تنظیم پلتفرم‌های آنلاین را که می‌توانند هم در مقاصد قانونی و هم در فعالیت‌های مضر، مانند سخنان نفرت‌انگیز و تروریسم، مورد استفاده قرار گیرند، مورد بررسی قرار می‌دهد. بررسی تأثیرات بالقوه پیشنهادهای اخیر در اصلاح بخش ۲۳۰ قانون شایستگی ارتباطات که در قبال محتوای تولیدشده توسط کاربران برای پلتفرم‌های آنلاین مصونیت قانونی قائل است.

علی‌رغم آن‌که پلتفرم‌هایی مانند فیس‌بوک و توییتر بستر انتشار سخنان نفرت‌انگیز و تبلیغات تروریستی را میسر کرده‌اند، اما برای ترویج جنبش‌های اجتماعی مثبت و ارزش‌های دموکراتیک نیز از آن‌ها استفاده شده است و به همین دلیل، در مقرره‌گذاری برای این پلتفرم‌ها باید ماهیت استفاده دوگانه آن‌ها را در نظر گرفته و از رویکردهای بیش‌ازحد گسترده یا محدودکننده اجتناب کرد.

در ماه‌های اخیر، مباحث زیادی در خصوص اصلاح بخش ۲۳۰ مطرح شده است. برخی از پیشنهادها مانند قانون PACT و قانون EARN IT از طریق مسئول نگه داشتن پلتفرم‌ها در قبال محتوای مضر به دنبال تقویت مقررات استفاده دومنظوره هستند، برخی پیشنهادهای دیگر مانند قانون SAFE TECH به دنبال لغو یا تضعیف شدید بخش ۲۳۰ هستند. باید توجه داشت که هر اصلاحی در بخش ۲۳۰ باید بین حفاظت از آزادی بیان و جلوگیری از انتشار آنلاین محتوای مضر تعادلی برقرار کند. این امر، مستلزم طراحی یک رویکرد دومنظوره و ترکیبی از اقدامات داوطلبانه، نظارت دولتی و مسئولیت قانونی است. پلتفرم‌ها باید تشویق شوند تا اقدامات داوطلبانه‌ای مانند سیاست‌های تعدیل محتوا و مکانیسم‌های گزارش‌دهی کاربر را جهت کمک به جلوگیری از انتشار محتوای مضر انجام دهند. دولت نیز باید برخی مکانیسم‌های نظارتی مانند کمیسیون‌های مستقل یا نهادهای استاندارد صنعتی را ایجاد کند تا از مدیریت مؤثر سخنان نفرت‌برانگیز و تبلیغات تروریستی توسط پلتفرم‌ها اطمینان حاصل شود.

قانون‌گذاران ایالتی نیازمند آن هستند تا اهمیت مقررات مؤثر برای استفاده دومنظوره در ترویج آزادی بیان، جلوگیری از سخنان نفرت‌انگیز و تبلیغات تروریستی و ترویج ارزش‌های دموکراتیک آنلاین را درک کنند. تنظیم مؤثر پلتفرم‌های آنلاین امری پیچیده و چالشی است، اما برای محافظت از مردم و ارتقای منافع عمومی ضروری است. در نتیجه، قانون‌گذاران و رهبران صنعت با در نظر گرفتن ماهیت استفاده دومنظوره این پلتفرم‌ها و تأثیرات بالقوه اصلاحات پیشنهادی بخش ۲۳۰، می‌بایست برای ایجاد چارچوبی جامع و مؤثر جهت تنظیم پلتفرم‌های دارای کاربرد دوگانه با یکدیگر همکاری کنند.

عنوان	Dual-use regulation: Managing hate and terrorism online before and after Section 230 reform
نویسنده	Brian Fishman
مرکز مطالعاتی	Brookings
تاریخ انتشار	March 14, 2023

تراشه

آنچه رهبران ایالتی و محلی باید در مورد طرح یارانه‌های نیمه‌هادی بایدن بدانند

این گزارش تلاش‌های دولت بایدن برای تقویت صنعت نیمه‌هادی آمریکا در پی مواجهه با افزایش رقابت جهانی و اختلالات زنجیره تأمین را مورد بحث قرار می‌دهد. این تلاش‌ها پیامدهای مهمی برای رهبران دولتی و محلی خواهد داشت، به‌ویژه در مناطقی که نیمه‌هادی‌ها به‌شدت مهم هستند.

این گزارش با ارائه یک مرور مختصر از صنعت نیمه‌هادی‌ها و اهمیت آن برای اقتصاد ایالات‌متحده به‌ویژه از نظر مشاغل پردرآمد و نوآوری آغاز می‌شود. سپس چالش‌های پیش روی صنعت ازجمله ظهور رقبای خارجی و همه‌گیری کرونا مورد بحث قرار می‌گیرد که زنجیره‌های تأمین را مختل و نیاز به تولید داخلی را بیش‌ازپیش پررنگ کرده است. بر همین اساس، پاسخ دولت بایدن به این چالش‌ها، به‌ویژه خبر اخیر در خصوص اختصاص ۵۲ میلیارد دلار بودجه برای صنعت نیمه‌هادی به‌عنوان بخشی از قانون سرمایه‌گذاری زیرساختی و مشاغل دوحزبی مورد بررسی قرار می‌گیرد. با توجه به بخش‌های مختلف این بودجه، مانند سرمایه‌گذاری در تحقیق و توسعه، تولید و توسعه نیروی کار، باید گفت که این بودجه گام مهمی در جهت تقویت صنعت نیمه‌هادی آمریکا و کاهش اتکا به تأمین‌کنندگان خارجی است. از آن‌جایی که سرمایه‌گذاری در تحقیق و توسعه بسیار مهم است، طرح دولت بایدن کمک می‌کند تا از پیشگامی ایالات‌متحده در نوآوری‌های مروبط به نیمه‌هادی اطمینان حاصل شود.

بااین‌حال، باید توجه داشت که صرف تخصیص بودجه برای رسیدگی به تمام چالش‌های پیش روی صنعت کافی نیست. سیاست‌گذاران باید به انعطاف‌پذیری زنجیره تأمین، حفاظت از مالکیت معنوی و روابط تجاری با رقبای خارجی نیز بپردازند. رهبران دولتی و محلی نقش مهمی در این تلاش‌ها دارند، به‌ویژه از نظر حمایت از سیاست‌هایی که از صنعت نیمه‌هادی در مناطق خود انجام می‌دهند.

این گزارش با ارائه توصیه‌هایی به رهبران دولتی و محلی برای حمایت از صنعت نیمه‌هادی به پایان می‌رسد. این توصیه‌ها شامل ایجاد مشارکت با ذی‌نفعان صنعت، سرمایه‌گذاری در نیروی کار و حمایت از سیاست‌هایی است که از صنعت حمایت می‌کند؛ مانند مشوق‌های مالیاتی و سرمایه‌گذاری‌های زیربنایی. این تلاش‌ها برای اطمینان از رهبری جهانی ایالات‌متحده در نوآوری و تولید نیمه‌هادی‌ها حیاتی خواهد بود.

عنوان	What state and local leaders need to know about Biden's semiconductor subsidies
نویسنده	Mark Muro, Joseph Parilla, Martha Ross
مرکز مطالعاتی	Brookings
تاریخ انتشار	March 2, 2023

اهمیت استراتژیک میراث تراشه‌ها

این گزارش بر نیاز به حفظ و نوسازی زیرساخت‌های موجود در ایالات‌متحده برای تراشه‌ها پافشاری می‌کند. این گزارش پیامدهای ژئوپلیتیکی کاهش عرضه تراشه‌های قدیمی را بررسی و اهمیت سرمایه‌گذاری در نوسازی این خطوط تولید را موردبحث قرار می‌دهد.

تراشه‌ها بخشی حیاتی در تقریباً تمام دستگاه‌های الکترونیکی، گوشی‌ها و خودروهای هوشمند و تجهیزات نظامی هستند. توانایی ایالات‌متحده برای تولید این تراشه‌ها در طول سالیان اخیر به دلیل عوامل مختلفی ازجمله بسته شدن کارخانه‌های تولیدی، افزایش هزینه‌های تولید و افزایش رقابت از سوی سازندگان خارجی، کاهش یافته است. این عوامل موجب اتکای بسیار به نیمه‌هادی‌های خارجی، به‌ویژه محصولات چین، شده است. حفظ و نوسازی زیرساخت‌های تولید تراشه‌ها در ایالات‌متحده برای امنیت ملی، رقابت اقتصادی و نوآوری‌های فناورانه بسیار مهم است. از سوی دیگر، باید اهمیت تراشه‌های قدیمی که کهنه و کمتر پیشرفته‌تر هستند، اما هنوز در بسیاری از برنامه‌های کاربردی مهم استفاده می‌شوند، نیز تبیین شود. **تراشه‌های قدیمی به‌ویژه برای وزارت دفاع آمریکا که در سیستم‌های تسلیحاتی خود شدیداً متکی به این تراشه‌ها است، مهم ارزیابی می‌شود. اتکای وزارت دفاع به این تراشه‌ها یعنی هرگونه اختلال در زنجیره تأمین می‌تواند عواقبی جدی برای امنیت ملی امریکا داشته باشد.**

ایالات‌متحده باید برای نوسازی زیرساخت‌های خود برای تولید تراشه‌ها به‌ویژه تراشه‌های قدیمی، سرمایه‌گذاری کند تا زنجیره تأمین قابل‌اعتمادی را بیافریند. این گزارش برخی اقدامات سیاستی برای دستیابی به این هدف را توصیه می‌کند، مثل مشوق‌های مالیاتی برای تولیدکنندگان تراشه، افزایش بودجه تحقیق و توسعه و تلاش برای تقویت زنجیره‌های تأمین داخلی. ضرورت افزایش همکاری بین دولت و بخش خصوصی برای رسیدگی به چالش‌های پیش روی صنعت تراشه و ایجاد بستر مشارکت‌های دولتی و خصوصی برای حمایت از تحقیق و توسعه و تدوین یک استراتژی ملی برای رسیدگی به چالش‌های این صنعت از موضوعات مهمی است که باید مورد توجه قرار بگیرد.

کاهش توانایی ایالات‌متحده برای تولید تراشه در داخل، پیامدهای ژئوپلیتیکی قابل ملاحظه‌ای دارد. چین باهدف تبدیل‌شدن به رهبر جهانی در این زمینه، سرمایه‌گذاری زیادی در صنعت نیمه‌هادی خود انجام داده است. توانایی ایالات‌متحده برای حفظ صنعت نیمه‌هادی قوی برای منافع اقتصادی و استراتژیک آن کشور حیاتی است.

عنوان	The Strategic Importance of Legacy Chips
نویسنده	Sujai Shivakumar, Charles Wessner, Thomas Howell
مرکز مطالعاتی	CSIS
تاریخ انتشار	March 3, 2023

سایر

هویت دیجیتالی بهبودیافته بدون هویت ملی

این گزارش نیاز به بهبود سیستم‌های هویت دیجیتال و تأثیر بالقوه آن‌ها بر حریم خصوصی و آزادی افراد را بررسی می‌کند. سیستم‌های هویت دیجیتال تنها درصورتی‌که با در نظر گرفتن حریم خصوصی و حقوق فردی طراحی شده باشند، می‌توانند مزایای متعددی مثل افزایش امنیت و کارایی ارائه دهند.

نویسنده با بحث در مورد چشم‌انداز کنونی سیستم‌های هویت دیجیتال آغاز شده و نشان می‌دهد با اینکه بسیاری از افراد از هویت‌های دیجیتال برای اهداف مختلف، مانند دسترسی به خدمات آنلاین و انجام تراکنش‌های مالی استفاده می‌کنند، هیچ استاندارد جهانی پذیرفته‌شده‌ای برای هویت دیجیتال وجود ندارد. این عدم استانداردسازی می‌تواند مدیریت هویت افراد را دشوار کرده و منجر به افزایش آسیب‌پذیری در برابر سرقت هویت و سایر اشکال تقلب شود. سپس این گزارش به بررسی مزایای بالقوه سیستم‌های هویت دیجیتالی بهبودیافته ازجمله افزایش امنیت، کارایی و راحتی می‌پردازد.

یک سیستم هویت دیجیتال با طراحی مناسب می‌تواند تقلب را کاهش، دسترسی به خدمات مالی و سایر خدمات آنلاین را افزایش و خدمات دولتی را ساده کند. بااین‌حال، خطرات بالقوه مرتبط با سیستم‌های هویت دیجیتال به‌ویژه از نظر حریم خصوصی و آزادی فردی نیز باید مورد توجه قرار بگیرد. سیستم‌های هویت دیجیتال با طراحی ضعیف می‌تواند برای جمع‌آوری و سوءاستفاده از داده‌های شخصی، نقض حقوق فردی، نظارت و دیگر اشکال کنترل دولتی مورداستفاده قرار گیرند.

برای رسیدگی به این خطرات، نویسنده چندین اصل کلیدی را برای توسعه سیستم‌های هویت دیجیتال توصیه می‌کند، ازجمله حفاظت از حریم خصوصی در مرحله طراحی، همراه با شفافیت و کنترل کاربر. سیستم‌های هویت دیجیتال باید حریم خصوصی و آزادی فردی را در نظر گرفته و افراد بر نحوه جمع‌آوری، ذخیره‌سازی و استفاده از داده‌های شخصی خود کنترل داشته باشند. استفاده از سیستم‌های هویت غیرمتمرکز که به افراد اجازه می‌دهد تا هویت دیجیتالی خود را کنترل کنند، می‌تواند یک جایگزین مناسب باشد، زیرا این سیستم‌های هویت غیرمتمرکز امنیت و حریم خصوصی و انعطاف‌پذیری و قابلیت حمل بیشتری دارند. نقش دولت‌ها در توسعه سیستم‌های هویت دیجیتال نیز از دیگر مضوعات مهمی است که باید مورد توجه قرار گیرد. دولت نقش اساسی در حصول اطمینان از طراحی سیستم‌های هویت دیجیتال با در نظر گرفتن حقوق و آزادی‌های فردی دارد، اما نباید تنها ارائه‌دهنده هویت دیجیتال باشد. در عوض، دولت باید با بازیگران بخش خصوصی همکاری کند تا برای هویت دیجیتال چارچوبی ایمن ایجاد کند که به حریم خصوصی و آزادی فردی هم احترام می‌گذارد.

عنوان	Improved Digital Identity Is National-ID-Free
نویسنده	Jim Harper
مرکز مطالعاتی	AEI
تاریخ انتشار	February 22, 2023

چگونه فناوری‌های حیاتی نسل بعدی را در اولویت قرار دهیم؟

این گزارش نیاز به یک استراتژی ملی برای توسعه و استقرار فناوری‌های حیاتی در رقابت رو به ازدیاد جهانی را مورد بحث قرار می‌دهد. این گزارش اولویت دادن به توسعه فناوری‌های نسل بعدی مانند هوش مصنوعی، محاسبات کوانتومی و بیوتکنولوژی برای حفظ رقابت‌پذیری ایالات‌متحده در بازار جهانی را برجسته کرده و تأکید می‌کند: **فناوری‌های حیاتی به یکی از ارکان اصلی امنیت ملی، رقابت اقتصادی و رفاه اجتماعی تبدیل شده‌اند. بااین‌حال، دولت ایالات‌متحده در حال حاضر از داشتن یک استراتژی منسجم برای توسعه و استقرار این فناوری‌ها که خطرات قابل‌توجهی را برای این کشور ایجاد می‌کند محروم است.**

نویسندگان رویکردی جامع برای اولویت‌بندی فناوری‌های حیاتی نسل بعدی پیشنهاد می‌کند که شامل اتخاذ یک استراتژی ملی برای نوآوری، سرمایه‌گذاری در تحقیقات پایه و افزایش همکاری بین بخش‌های دولتی و خصوصی است. **هوش مصنوعی، محاسبات کوانتومی و بیوتکنولوژی** سه مورد از حیاتی‌ترین فناوری‌های نسل بعدی است و ایالات‌متحده باید رهبر توسعه و استقرار این فناوری‌ها باشد، در غیر این صورت خطر عقب افتادن از چین و سایر کشورهایی که در این زمینه‌ها سرمایه‌گذاری زیادی می‌کنند، وجود خواهد داشت. برهمین اساس، دولت آمریکا باید بودجه تحقیقات پایه در این زمینه‌ها را افزایش دهد و مشارکت بین دانشگاه‌ها، دولت فدرال و صنعت را برای پیشبرد نوآوری افزایش دهد.

اهمیت حمایت از استعدادهای داخلی برای حمایت از توسعه فناوری‌های حیاتی از نکات مهمی است که مورد تأکید قرار می‌گیرد. دولت برای این منظور موظف است تا بودجه برای برنامه‌های آموزشی STEM[1] و توسعه نیروی کار را بالا ببرد و سیاست‌های مهاجرتی جدیدی را برای جذب و حفظ استعدادهای برتر از سراسر جهان اتخاذ کند. از سوی دیگر، دولت برای مقابله با خطرات و چالش‌های ناشی از فناوری‌های نوظهور چارچوب‌های نظارتی جدیدی را باید ایجاد کند. بسیاری از فناوری‌های حیاتی، مانند هوش مصنوعی و بیوتکنولوژی، پتانسیل تأثیرگذاری بالایی بر جامعه داشته و مسائل اخلاقی، قانونی و اجتماعی را مطرح می‌کنند؛ بنابراین دولت باید برای تدوین مقررات جدیدی که بین نیاز به نوآوری و نیاز به امنیت عمومی و ملاحظات اخلاقی تعادل برقرار می‌کند، با صنعت و جامعه مدنی همکاری کند.

۱. Science, technology, engineering, and mathematics

عنوان	How to Prioritize the Next Generation of Critical Technologies
نویسنده	Connor Fairman, Guest Contributor
مرکز مطالعاتی	CFR
تاریخ انتشار	February 23, 2023

بهینه‌سازی زنجیره تأمین آمریکای شمالی در فناوری‌های حیاتی

توافقنامه ایالات‌متحده، مکزیک و کانادا[۱] یک توافق تجاری است که در سال ۲۰۱۸ امضا شده و در سال ۲۰۲۰ به اجرا درآمد و جایگزین توافقنامه تجارت آزاد آمریکای شمالی[۲] شد. فصل ۶ این توافقنامه مربوط به جریان داده‌ها و فناوری‌های حیاتی است و گزارش اندیشکده بروکینگز پیامدهای این فصل و تأثیر بالقوه آن بر تجارت و نوآوری در اقتصاد دیجیتال را بررسی می‌کند. هدف از فصل ۶ این توافقنامه تسهیل جریان آزاد داده‌ها در سراسر این کشورها و تضمین حریم خصوصی و امنیت داده‌ها است. این فصل شامل مقرراتی در مورد حفاظت از فناوری‌های حیاتی نیز هست که به‌عنوان فناوری‌هایی برای امنیت ملی یا عملکرد زیرساخت‌های حیاتی ضروری هستند.

این توافق می‌تواند مزایای بسیاری برای ایالات‌متحده داشته باشد، زیرا این کشور خاستگاه بسیاری از شرکت‌های فناوری پیشرو جهان و صادرکننده عمده خدمات دیجیتال است. این توافق می‌تواند برای مکزیک و کانادا هم از طریق دسترسی بیشتر آن‌ها به بازار ایالات‌متحده و تشویق نوآوری و سرمایه‌گذاری در اقتصادهای دیجیتالی‌شان نافع باشد.

بااین‌حال، این گزارش برخی چالش‌ها و خطرات بالقوه مرتبط با فصل ۶ این توافقنامه را نیز شناسایی می‌کند. یکی از نگرانی‌های اصلی، پتانسیل الزامات محلی سازی داده‌ها است که جریان آزاد داده‌ها و مزایای توافق را محدود کند. به همین منظور، ضروری است تا این سه کشور با یکدیگر همکاری کنند تا از بومی‌سازی حداقلی و ضروری داده‌ها اطمینان حاصل شود و اهداف توافق تضعیف نشود.

نگرانی دیگر احتمال محدودیت در انتقال فناوری‌های حیاتی است. اگرچه چنین محدودیت‌هایی برای امنیت ملی مهم هستند، اما می‌توانند نوآوری و رقابت در اقتصاد دیجیتال را نیز محدود کنند. به توصیه این گزارش ایالات‌متحده، مکزیک و کانادا باید با همدیگر همکاری کنند تا از ضروری و متناسب بودن هرگونه محدودیت در فناوری‌های حیاتی اطمینان حاصل کرده و تجارت یا نوآوری را محدود نکنند.

۱. United States-Mexico-Canada Agreement
۲. North American Free Trade Agreement

عنوان: Optimizing North American supply chains in critical technologies: The USMCA digital advantage
نویسنده: Dan Ciuriak
مرکز مطالعاتی: Brookings
تاریخ انتشار: February 2023

چگونه دره سیلیکون سرکوب اعتراضات چین را مهندسی کرد؟

این گزارش به نحوه همکاری شرکت‌های فناوری دره سیلیکون با دولت چین برای سرکوب مخالفان و با استفاده از ابزارهای نظارتی، فیلتر اینترنت و فناوری‌های ردیابی مکان به‌طور غیرمستقیم می‌پردازد. گزارش نشان می‌دهد این ابزارها در سرکوب اعتراضات طرفداران دموکراسی و صدای مخالف حزب کمونیست چین مؤثر بوده است. علی‌رغم اظهارات عمومی این شرکت‌های فناوری در مورد ترویج آزادی بیان و حمایت از دموکراسی، فعالیت‌های آن‌ها در پشت‌صحنه به افزایش استبداد در چین کمک کرده است، چرا که تمرکز شرکت‌ها بر سود خود و دسترسی به بازار چین باعث شده که عواقب استفاده از فناوری‌ها برای نظارت و سرکوب فعالان حقوق بشر و معترضان چینی را نادیده بگیرند. نویسنده نمونه‌هایی از نحوه ارائه فناوری و خدمات شرکت‌هایی مانند گوگل، اپل و سیسکو به دولت چین را نشان می‌دهد که امکان نظارت، سانسور و ردیابی فعالیت‌های شهروندان چینی را فراهم کرده است. **به‌عنوان نمونه، گوگل یک موتور جستجوی سانسور شده برای چین ایجاد کرده است، اپل برنامه‌هایی که ارتباط مخالفان را میسر می‌کند، حذف کرده است. همکاری سیسکو با چین در ایجاد یک سیستم نظارتی موسوم به «سپر طلایی»، امکان نظارت بر فعالیت‌های آنلاین در زمان واقعی را فراهم می‌کند.**

در پایان، نویسنده خواستار پاسخگویی بیشتر از شرکت‌های دره سیلیکون برای فعالیت‌هایشان در چین است و پیشنهاد می‌کند که سیاست‌گذاران پیامدهای حقوق بشری این فناوری‌ها را در نظر بگیرند. بر همین اساس، دولت‌ها و جامعه مدنی باید برای ایجاد چارچوبی در توسعه و استقرار فناوری اخلاقی و با تمرکز بر حمایت از حقوق بشر و ارزش‌های دموکراتیک با یکدیگر مشارکت کنند.

عنوان	How Silicon Valley Engineered China's Protest Crackdowns
نویسنده	Craig Singleton
مرکز مطالعاتی	FDD
تاریخ انتشار	March 3, 2023

آشفتگی سیاسی و اقتصادی پاکستان خطرات محدود کردن آزادی‌های دیجیتال را می‌افزاید

این گزارش به بررسی چالش‌های آزادی دیجیتال در پاکستان در بحبوحه بحران‌های سیاسی و اقتصادی این کشور پرداخته و تلاش‌های دولت پاکستان برای تنظیم رسانه‌های اجتماعی و اینترنت و چگونگی تأثیر این تلاش‌ها بر آزادی بیان، دسترسی به اطلاعات و حقوق بشر در این کشور را بررسی می‌کند. دولت پاکستان اقدامات مختلفی را برای محدود کردن آزادی‌های دیجیتال انجام داده است، ازجمله اجرای قانون پیشگیری از جرائم الکترونیکی[1] (PECA) مصوب سال ۲۰۱۶ که برای هدف قرار دادن روزنامه‌نگاران، فعالان و مدافعان حقوق بشر استفاده شد. در چند سال گذشته آزار و اذیت، ارعاب و خشونت علیه خبرنگاران از طریق حملات سایبری و تهاجم فیزیکی افزایش یافته و دولت پاکستان از تاکتیک‌های مختلفی، ازجمله مسدود کردن وب سایت‌ها و پلتفرم‌های رسانه‌های اجتماعی، برای محدود کردن دسترسی به اطلاعات استفاده کرده است.

تمرکز دولت بر تثبیت اقتصاد باعث بی‌توجهی به ترویج و حفاظت از آزادی‌های دیجیتال شده است. این امر محیطی را ایجاد کرده که در آن سانسور آنلاین، نظارت و جرائم سایبری در حال افزایش است. این گزارش با بحث در مورد نیاز به حمایت بین‌المللی برای ترویج و حفاظت از آزادی‌های دیجیتال در پاکستان به پایان می‌رسد و از جامعه بین‌المللی، سازمان‌های جامعه مدنی، رسانه‌ها و شرکت‌های فناوری می‌خواهد تا با همکاری یکدیگر از پایبندی دولت پاکستان به تعهدات خود در قبال حقوق بشر و آزادی بیان، علی‌الخصوص در فضای دیجیتال، اطمینان حاصل کنند.

۱. The Prevention of Electronic Crimes Act

عنوان	Amid Pakistan's political and economic turmoil, risks to curbs on digital freedoms grow
نویسنده	Uzair Younus
مرکز مطالعاتی	Atlanticcouncil
تاریخ انتشار	March 6, 2023

گسترش استفاده از فناوری برای مدیریت مهاجرت

این گزارش به موضوع استفاده از فناوری برای مدیریت مهاجرت که به یک موضوع مهم و تهدید امنیت ملی در دنیای مدرن تبدیل شده تمرکز دارد. بر همین اساس، می‌توان از فناوری برای بهبود کارایی و اثربخشی مدیریت مهاجرت، کاهش هزینه آن و افزایش امنیت استفاده کرد.

این گزارش با ارائه وضعیت کلی چالش‌های پیش روی مدیریت مهاجرت و نقشی که فناوری می‌تواند در رسیدگی به این چالش‌ها داشته باشد، آغاز می‌شود. فناوری می‌تواند برای بهبود کارایی مدیریت مرز، ارائه داده‌های دقیق‌تر در مورد جریان‌های مهاجرتی، افزایش اثربخشی مدیریت مهاجرت و حمایت از ادغام مهاجران در جامعه مورد استفاده قرار گیرد. استفاده از سیستم‌های شناسایی بیومتریک، گیت‌های الکترونیکی و مرزهای هوشمند در کشورهای مختلف در جهان همچنین استفاده از رسانه‌های اجتماعی و سایر فناوری‌های دیجیتال برای حمایت از ادغام مهاجران در جامعه از موضوعات مهمی است که در خصوص آن بحث می‌شود. در مقابل، تحلیلی از چالش‌ها و خطرات مرتبط با استفاده از فناوری برای مدیریت مهاجرت نیز ارائه می شود. باید توجه داشت که برخی خطرات بالقوه در این خصوص نیز وجود دارد، مثل احتمال نقض حریم خصوصی، نقض داده‌های محافظت شده و سوءاستفاده از فناوری توسط سازمان‌های دولتی. نویسندگان بر نیاز به همکاری بین‌المللی بهتر برای رسیدگی به این خطرات و استفاده از فناوری در مدیریت مهاجرت مطابق با استانداردهای بین‌المللی حقوق بشر تأکید دارند و پیشنهادهایی را برای چگونگی استفاده از فناوری برای مدیریت مهاجرت به شیوه‌ای مؤثر و کارآمدتر ارائه می‌دهند.

عنوان	The Expanding Use of Technology to Manage Migration
نویسنده	Marti Flacks, Erol Yayboke, Lauren Burke, Anastasia Strouboulis
مرکز مطالعاتی	CSIS
تاریخ انتشار	March 6, 2023

پایان

زاویه
نگاهی نو،
به حکمرانی فضای مجازی

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