معماری جهانی حاکمیت دیجیتال

عنوان: معماری جهانی حاکمیت دیجیتال: تحلیل مقایسه‌ای مدل‌های سانسور و کنترل اینترنت در سال ۲۰۲۵

نویسنده: NOX

چکیده:

این مقاله به بررسی تکامل روش‌های سانسور و کنترل اینترنت در کشورهای کلیدی تا سال ۲۰۲۵ می‌پردازد. تحلیل ارائه شده بر اساس رویکردی تطبیقی است و سه مدل مسلط را شناسایی می‌کند: مدل اقتدارگرا-حاکمیتی (چین، روسیه، ایران، کره شمالی)، مدل لیبرال-تنظیم‌گر (ایالات متحده، اتحادیه اروپا، اسرائیل) و مدل ترکیبی (ترکیه، مصر و چندین کشور در آسیا، آفریقا و آمریکای لاتین). استدلال می‌شود که تا سال ۲۰۲۵، مفهوم «اینترنت حاکمیتی» از یک ایده نظری به یک معماری عینی تکنیکی-حقوقی تبدیل شده که از سوی شمار زیادی از دول‌ها پیاده‌سازی شده است. تمرکز مقاله بر ابزارهای تکنولوژیک (DPI، هوش مصنوعی)، چارچوب‌های حقوقی و اهداف ژئوپلیتیک پشت این محدودیت‌ها است. مقاله با نتیجه‌گیری در مورد تشدید چندپارگی اینترنت جهانی («اسپلینترنت») و شکل‌گیری اکوسیستم‌های دیجیتال تابآور که توسط قواعد خود اداره می‌شوند، به پایان می‌رسد.

کلیدواژه‌ها: سانسور اینترنت، حاکمیت دیجیتال، ۲۰۲۵، بازرسی عمقی بسته‌های اطلاعاتی (DPI)، هوش مصنوعی، مقررات‌گذاری، حقوق بشر، امنیت سایبری.

مقدمه

تا سال ۲۰۲۵، اینترنت دیگر یک فضای جهانی یکپارچه همان‌گونه که در ابتدا تصور می‌شد، نیست. تحت تأثیر تنش‌های ژئوپلیتیک، نگرانی‌های امنیت ملی و تمایل برای حاکمیت فرهنگی، مدل‌های ملی و منطقه‌ای مختلفی برای کنترل قلمرو اطلاعات دیجیتال ظهور کرده‌اند. اصطلاح «سانسور» تکامل یافته تا نه تنها شامل مسدودسازی محتوا، بلکه یک سیستم پیچیده از moderation پیشگیرانه، فشار قانونی بر پلتفرم‌ها، دستکاری ترافیک و اطلاعاترسانی هدفدار نادرست نیز بشود.

هدف این مقاله، انجام یک تحلیل مقایسه‌ای از مدل‌های کنترل اینترنت در قدرت‌های بزرگ جهانی، شناسایی ویژگی‌های مشترک و تفاوت‌های اساسی آن‌ها و ارزیابی تأثیرشان بر حقوق شهروندی، اقتصاد دیجیتال و ثبات بین‌المللی است.

۱. روش‌شناسی

این پژوهش بر اساس یک تحلیل کیفی تطبیقی استوار است. کشورها بر اساس تأثیرشان بر سیاست دیجیتال جهانی و نمایندگی مدل‌های مختلف کنترل، انتخاب شدهاند. منابع مورد استفاده شامل موارد زیر است:

- اسناد قانونی ملی (قوانین مربوط به «اینترنت حاکمیتی»، حفاظت از داده، ضدیت با افراطی‌گری)؛
- گزارش‌های سازمان‌های بین‌المللی (خانه آزادی، گزارشگران بدون مرز، Access Now)؛

- گزارش‌های فنی شرکت‌های امنیت سایبری (سیتیزن لب، پالو آلتو نتورکس)؛
- بیانیه‌های عمومی مقامات دولتی و نهادهای تنظیم‌گر.

۲. تحلیل مقایسه‌ای مدل‌های کنترل اینترنت

۲.۱. مدل اقتدارگرای حاکمیت دیجیتال

چین:
تا سال ۲۰۲۵، دیوار آتشین بزرگ چین (GFW) به یک سیستم جامع مدیریت جامعه دیجیتال با نام «اعتبار اجتماعی ۲.۰» تکامل یافته است. مسدودسازی مبتنی بر DPI با الگوریتم‌های پیش‌بینیکننده هوش مصنوعی تکمیل شده که قادرند discussions «نامطلوب» را در مراحل اولیه شناسایی و سرکوب کنند. تمام پلتفرم‌های اصلی جهانی با جایگزین‌های داخلی (ویچت، دوبین، بایدو) که تحت کنترل کامل دولت هستند، جایگزین شده‌اند. صادرات این مدل — به‌ویژه از طریق ابتکار کمربند و جاده به کشورهای آفریقایی و آسیایی — به یک ابزار کلیدی قدرت نرم تبدیل شده است.

روسیه:
اجرای قانون «اینترنت حاکمیتی» (۲۰۱۹) تکمیل شده است. تا سال ۲۰۲۵، یک سیستم ملی نام دامنه (DNS) عملیاتی است که امکان جداسازی بخش اینترنت روسیه (رونت) از شبکه جهانی در مواقع ضروری را فراهم می‌کند. از DPI به‌طور فعال برای سرکوب VPNها و ترافیک رمزگذاری شده استفاده می‌شود. اهداف اصلی سانسور، انتقاد از مقامات، عملیات نظامی، محتوای LGBTQ+ و رسانه‌های مستقل هستند. مبانی قانونی شامل قوانین مربوط به «اخبار جعلی»، «عوامل خارجی» و «افراطی‌گری» می‌شود.

ایران:
مدل ایران، کنترل فنی را با سرکوب شدید ترکیب می‌کند. این کشور یکی از پیشرفته‌ترین سیستم‌های فیلترینگ محتوا در جهان را حفظ کرده که قادر است during protests پیامرسان‌ها (تلگرام، واتس‌اپ) و رسانه‌های اجتماعی را به صورت پویا مسدود کند. تا سال ۲۰۲۵، شناسایی اجباری کاربر برای دسترسی به وای‌فای و خرید سیم‌کارت الزامی است. کاهش پهنای باند اینترنت به سطحی بحرانی، during unrest معمولاً practiced می‌شود.

کره شمالی:
به عنوان معیار کنترل توتالیتر باقی مانده است. شبکه داخلی Kwangmyong کاملاً از اینترنت جهانی جدا است. دسترسی به اینترنت بین‌المللی به یک قشر نخبه محدود محدود شده است. محتوا به تبلیغات دولتی، مطالب ایدئولوژیک و اطلاعات علمی بسیار محدود، محدود شده است.

۲.۲. مدل لیبرال-تنظیم‌گری (ایالات متحده، اتحادیه اروپا، اسرائیل)

ایالات متحده: سانسور سنتی دولتی وجود ندارد، اما یک سیستم پیچیده از تنظیم‌گری خصوصی و عمومی شکل گرفته است. تحت فشار عمومی و نظارت FCC و FTC، پلتفرم‌های اصلی (متا، اکس، گوگل) سیاست‌های moderation خود را در مورد سخن نفرت‌پراکن، اطلاعات نادرست و تحریک به خشونت سخت‌تر کرده‌اند. یک بحث محوری در سال ۲۰۲۵ حول **بخش ۲۳۰** می‌گردد، قانونی که به پلتفرم‌ها مصونیت در قبال محتوای تولیدشده توسط کاربر می‌دهد. دعوت‌ها برای لغو یا اصلاح آن، پلتفرم‌ها را به سانسور پیش‌دستانه برای اجتناب از ریسک‌های قانونی سوق می‌دهد. بنابراین، سانسور به صورت مؤثری به شرکت‌های خصوصی تفویض شده است. **اتحادیه اروپا:** اتحادیه اروپا پیشرفته‌ترین چارچوب تنظیم‌گری در جهان را توسعه داده است که در عمل استانداردهای جهانی را تعیین می‌کند. سانسور غیرمستقیم است و از طریق الزام به رعایت قوانین اعمال می‌شود: • GDPR: مسدودسازی سایت‌هایی که الزامات حفاظت از

داده را نقض می‌کنند؛ • Digital Services Act (DSA): پلتفرم‌ها موظفند محتوای غیرقانونی (مانند تروریسم، سخن نفرت‌پراکن) را تحت تهدید جریمه‌های کلان فوراً حذف کنند؛ • Digital Markets Act (DMA): پلتفرم‌های انحصاری را هدف قرار می‌دهد. اتحادیه اروپا در مسدودسازی در سطح دولتی engaged نمی‌شود، بلکه یک محیط قانونی ایجاد می‌کند که در آن عدم رعایت مقررات منجر به اخراج de facto از بازار می‌شود. **اسرائیل:** اسرائیل موردی منحصر به فرد از مدل لیبرال-تنظیم‌گری را ارائه می‌دهد که تأکید شدیدی بر امنیت ملی دارد. به عنوان یک دموکراسی با فناوری پیشرفته، اسرائیل عموماً به اصول اینترنت باز پایبند است. با این حال، در میانه مناقشه جاری و تهدیدات امنیتی، سانسور به صورت گزینشی و بر اساس مبانی قانونی مستدل اعمال می‌شود. • **چارچوب قانونی:** ابزار اصلی، سانسور نظامی است که از دوران تأسیس دولت به ارث رسیده است. تمامی رسانه‌ها و نشریات آنلاین باید مطالب مرتبط با امنیت را برای بررسی پیشین توسط **اداره سانسور نظامی** ارسال کنند. تا سال ۲۰۲۵، این اصل برای عصر دیجیتال adapt شده است. • **فناوری و عمل:** مقامات می‌توانند از ارائه‌دهندگان خدمات اینترنت (ISPs) و پلتفرم‌های اجتماعی درخواست کنند محتوایی را که تهدیدی برای امنیت ملی یا تحریک‌کننده خشونت تلقی می‌شود، حذف کنند. این تصمیمات frequently در دیوان عالی کشور به چالش کشیده می‌شوند که به عنوان یک ضدمتقابل حیاتی عمل می‌کند. در دوران تشدید نظامی‌گری، سانسور تشدید می‌شود و پلتفرم‌ها تحت فشار فزایندهای برای compliance قرار می‌گیرند. بر خلاف رژیم‌های اقتدارگرا، اسرائیل یک جامعه مدنی پرجنب‌وجوش و مطبوعات آزاد دارد که تصمیمات سانسور را به چالش می‌کشند و فرآیند را شفاف‌تر می‌سازند.

۲.۳. مدل ترکیبی (ترکیه، مصر، آسیا، آفریقا، آمریکای لاتین)

ترکیه: یکی از بزرگترین فهرست‌های محتوای مسدودشده در جهان را تحت قوانین حافظ منافع دولتی و نظم عمومی حفظ می‌کند. **قانون شماره ۵۶۵۱** در سال ۲۰۲۵ تقویت شد و به تنظیم‌گر BTK این امکان را می‌دهد که هر محتوایی را within چهار ساعت و بدون حکم دادگاه مسدود کند. **قانون شماره ۷۴۱۶** پلتفرم‌ها را تحت فشار قرار می‌دهد تا representatives محلی تعیین کنند و از دستورالعمل‌های دولتی تبعیت کنند، که در آن از throttling به صورت progressive تا اختلال کامل خدمات استفاده می‌شود. **مصر:** از مجوزدهی telecom به عنوان ابزار کنترل استفاده می‌کند. مسدودسازی VPNها و برنامه‌های encrypted (مانند سیگنال) یک اقدام standard است. در خلال تنش‌های سیاسی، shutdownهای اینترنتی در سطح ملی ممکن است رخ دهد. قوانین جرایم سایبری اختیارات گستردهای برای مسدود کردن سایت‌ها و نظارت بر شهروندان اعطا می‌کنند. **آسیا (هند و ویتنام):** هند under بهانه ایمنی عمومی، به صورت routine shutdownهای منطقه‌ای اینترنت اعمال می‌کند. قوانین IT به دولت اختیارات گستردهای برای مسدودسازی می‌دهند. ویتنام از مدل چینی تقلید می‌کند و از شرکت‌های فناوری می‌خواهد داده‌های کاربران را به صورت محلی ذخیره کنند، upon درخواست به اشتراک بگذارند و محتوا را ۲۴ within ساعت حذف کنند. **آفریقا:** دولت‌های اتیوپی، اوگاندا و زیمبابوه به طور فزایندهای از shutdownهای اینترنتی در during انتخابات و اعتراضات استفاده می‌کنند. فناوری و مدل‌های کنترل چینی — که often با زیرساخت‌های هواوی و ZTE bundle شده‌اند — در حال gaining نفوذ هستند. **آمریکای لاتین:** تا سال ۲۰۲۵، این region روندهای mixed را نشان می‌دهد که عمدتاً با model ترکیبی و با variations قابل توجه مطابقت دارد. • **برزیل:** به عنوان بزرگترین اقتصاد منطقه، برزیل سعی می‌کند آزادی بیان را با مبارزه against اطلاعات نادرست و جرایم سایبری متعادل کند. **Marco Civil da Internet** با الهام از اتحادیه اروپا، همچنان سنگ بنای تنظیم‌گری باقی می‌ماند. با این حال، دستورات فزاینده دادگاه برای مسدود کردن messengers پرطرفدار (مانند واتس‌اپ و تلگرام) به دلیل امتناع از ارائه داده‌های کاربر یا curb کردن اخبار جعلی، debateهایی را برانگیخته است. سانسور often targeted و موقت است اما از نظر تناوب در حال رشد است. • **ونزوئلا و نیکاراگوئه:** به سمت مدل‌های اقتدارگرا حرکت می‌کنند. دولت‌ها از ابزارهای فنی برای مسدود کردن سایت‌های خبری مستقل و پلتفرم‌های اجتماعی، especially در during ناآرامی‌های سیاسی استفاده می‌کنند. **Conatec** (مرکز ملی کنترل فضای مجازی) ونزوئلا

سانسور را هماهنگ می‌کند. قوانین harsh جرایم سایبری، انتقاد آنلاین از دولت را جرم‌زدایی می‌کنند. • **کوبا:** نزدیک به کنترل کامل دولتی. اگرچه دسترسی به اینترنت تا سال ۲۰۲۵ گسترش یافته است، اما همچنان گران و به شدت regulated است. انحصار دولتی ETECSA telecom، فیلتر کردن محتوا و نظارت بر کاربران را امکان‌پذیر می‌سازد. انتقاد از دولت و دسترسی به رسانه‌های مستقل به صورت routinely مسدود می‌شوند.

۳. بحث و نتیجه‌گیری‌ها

تا سال ۲۰۲۵، جهان از اینترنت یکپارچه به مجموعه‌ای از قلمروهای دیجیتال ملی و منطقه‌ای fragmented — موسوم به اسپلینترنت — گذار کرده است. روندهای کلیدی شامل موارد زیر است: • **پیشرفته‌شدن فناوری:** مسدودسازی ساده محتوا جای خود را به سیستم‌های مبتنی بر DPI و هوش مصنوعی داده که قادر به moderation پیش‌بینانه و سرکوب دقیق ابزارهای دور زدن هستند. • **استتار قانونی:** سانسور increasingly از طریق ضدیت با افراطی‌گری، حفاظت از داده‌ها (اتحادیه اروپا)، یا حاکمیت و امنیت (روسیه، چین، اسرائیل) توجیه می‌شود که به آن legitimateبودن perceived در عرصه بین‌المللی می‌بخشد. • **خصوصی‌سازی سانسور:** در دموکراسی‌های لیبرال (آمریکا، اتحادیه اروپا)، نقش سانسورگر از دولت به شرکت‌ها منتقل شده است که تحت تهدید مجازات‌ها مجبور به پیروی از دستورات regulatory هستند. اسرائیل سانسور دولتی را حفظ کرده، اما در چارچوب‌های امنیتی محدود و با نظارت قضایی. • **بعد ژئوپلیتیک:** دو مدل جهانی در حال رقابت هستند: رویکرد regulatory آمریکا و اتحادیه اروپا (مبتنی بر حقوق و هنجارهای بازار) در مقابل مدل چین و روسیه (کنترل دولتی و انزوا). دولت‌های ترکیبی — به ویژه در آمریکای لاتین — بسته به شرایط سیاسی، عناصری از هر دو را به کار می‌گیرند. خطر در ایجاد حباب‌های اطلاعاتی پایدار، افزایش اقتدارگرایی و کاهش تبادل دانش فرامرزی نهفته است. همان‌گونه که مورد اسرائیل نشان می‌دهد، کشمکش بین openness و امنیت ملی، تناقض محوری است که آینده اینترنت را شکل می‌دهد.

پیوست: DPI و رهگیری گواهی

Deep Packet Inspection (DPI) یک فناوری تحلیل ترافیک است که به ارائه‌دهندگان یا بازیگران دولتی اجازه می‌دهد نه تنها ببینند شما به کجا متصل می‌شوید، بلکه محتوای واقعی بسته‌های داده را نیز بازرسی کنند. این امر، رفتار کاربر — تماشای ویدیو، استفاده از VPNها، ارسال پیام، دسترسی به Tor و غیره — را آشکار می‌سازد. در عمل، DPI امکان موارد زیر را فراهم می‌کند: • مسدودسازی یا throttling سرویس‌های خاص؛ • دور زدن ناشناس‌بودن VPN یا Tor؛ • نظارت بر رفتار آنلاین؛ • سانسور انبوه — حتی درون ترافیک encrypted. شدیدترین تهدید، در تضعیف اعتماد به فناوری‌های بنیادین اینترنت نهفته است. در بسیاری از کشورها، تحت بهانه مبارزه با تروریسم، محافظت از کودکان، اجرای تحریم‌ها، یا انگیزه‌های مشابه، دولت‌ها، ارائه‌دهندگان خدمات اینترنت (ISPs) را مجبور به پیاده‌سازی DPI و معرفی مراجع صدور گواهی (CAs) خود می‌کنند. این CAs می‌توانند گواهی‌های HTTPS جعلی صادر کنند — کاربران متوجه نمی‌شوند، مرورگرها هشدار نمی‌دهند و ترافیک از یک گره تحت کنترل عبور می‌کند. اتصال به ظاهر «امن» باقی می‌ماند، اما دولت می‌تواند legally ترافیک را — بدون هک کردن — با ربودن زیرساخت اعتماد، بخواند، ضبط کند و تغییر دهد. این عمل به عنوان **رهگیری گواهی** شناخته می‌شود و در ترکیب با DPI، یک سیستم نفوذ قانونی را تشکیل می‌دهد. چنین مکانیسم‌هایی بی‌طرفی شبکه، حریم خصوصی و خود ایده ارتباطات امن را نقض می‌کنند. هنگامی که دولت جایگزین اعتماد می‌شود — دیگر محافظت نمی‌کند. کنترل می‌کند.