آکادمی الزامات فناوری اطلاعات و ارتباطات برای مدیران ارشد دولتی

سرفصل

۵

نظارت بر اینترنت

UNITED NATIONS
APCICT - ESCAP

به نام خدا

آکادمی الزامات فناوری اطلاعات و ارتباطات برای مدیران

ارشد دولتی

سرفصل ۵:

نظارت بر اینترنت

(ویرایش اول)

فهرست مطالب

آکادمی الزامات فناوری اطلاعات و ارتباطات برای مدیران ارشد دولتی

سرفصل ۵: نظارت بر اینترنت

Contact:
United Nations Asian and Pacific Training Centre for Information
and Communication Technology for Development (UN-APCICT/ESCAP)
Bonbudong, 3rd Floor Songdo Techno Park
7-50 Songdo-dong, Yeonsu-gu, IncheonCity
Republic of Korea

Tel: 82 32 245 1700-02
Fax: 82 32 245 7712
E-mail: info@unapcict.org
http://www.unapcict.org

ISBN: 978-89-97748-02-0

Design and Layout: Scand-Media Corp., Ltd.
Printed in: Republic of Korea

پیشگفتار

دنیای امروزه، به خاطر توسعه سریع فناوری‌های اطلاعاتی و ارتباطی به هم مرتبط و سریعاً در حال تغییر است. طبق اعلام مجمع اقتصاد جهانی[1]، این فناوری‌ها، سیستم عصبی مشترک ما را نمایش می‌دهند، با راه‌حل‌های سازش‌پذیر، خلاق و هوشمند، با تار و پود زندگی تنیده می‌شوند، به ما کمک می‌کنند و توسعه پایدار و جامع‌تری را رواج می‌دهند.

دسترسی بیشتر به دانش و اطلاعات از طریق توسعه فناوری اطلاعات و ارتباطات، پتانسیل بهبود چشمگیر در معاش افراد فقیر و حاشیه‌ای دارد و برابری جنسیتی را ارتقا می‌دهد. فناوری‌های اطلاعاتی و ارتباطی با ارائه ابزارها و پلت‌فرم‌های مطمئن، شفاف و کارآمد، ارتباطات و همکاری می‌توانند پلی باشند که مردم کشورها و بخش‌های مختلف منطقه و فراتر از آن را به یکدیگر پیوند دهند. فناوری‌های اطلاعاتی و ارتباطی برای این ارتباط ضروری هستند و تبادل مؤثر کالا و خدمات را تسهیل می‌کنند. ماجراهای موفقیت منطقه آسیا و اقیانوسیه بسیار زیاد است: نوآوری‌های دولت الکترونیکی در حال بهبود دسترسی و کیفیت خدمات عمومی هستند. تلفن‌های همراه در حال درآمدزایی و فرصت‌های حرفه‌ای برای زنان هستند و صدای افراد آسیب‌پذیر به‌واسطه قدرت رسانه‌های اجتماعی بلندتر از گذشته به گوش می‌رسد.

هرچند، شکاف دیجیتالی در آسیا و اقیانوسیه هنوز یکی از گسترده‌ترین شکاف‌ها در جهان به شمار می‌رود، این حقیقت که کشورهای این منطقه در سرتاسر طیف کلی رتبه‌بندی شاخص جهانی توسعه فناوری اطلاعات و ارتباطات قرار گرفته‌اند، گواهی بر این ادعاست. برخلاف نفوذ تأثیرگذار تکنولوژیک و تعهدات بسیاری از بازیگران اصلی این منطقه، دسترسی به ارتباطات اساسی هنوز برای همگان تضمین نمی‌شود.

به‌منظور تکمیل پل ارتباطی شکاف دیجیتالی، سیاست‌گذاران باید متعهد شوند، پتانسیل فناوری‌های اطلاعاتی و ارتباطی را برای توسعه جامع اقتصادی و اجتماعی منطقه بیشتر بشناسند. به این منظور، مرکز آموزش توسعه به کمک فناوری اطلاعات و ارتباطات، در منطقه آسیا و اقیانوسیه (APCICT) مؤسسه منطقه‌ای UN/ESCAP را در تاریخ ۱۶ ژوئن ۲۰۰۶، با دستور کار تقویت تلاش‌های ۶۲ عضو ESCAP و کشورهای عضو وابسته از فناوری اطلاعات و ارتباطات در توسعه اقتصادی و اجتماعی‌شان از طریق توسعه ظرفیت انسانی مؤسساتی تأسیس کرد. این دستور کار پاسخی به بیانیه اصول و طرح قانون اجلاس جهانی جامعه اطلاعاتی (WSIS) است که بیان می‌کند: «هر

1- World Economic Forum

شخص باید فرصت آشنایی با مهارت‌ها و دانش لازم را داشته باشد، تا در جامعه اطلاعاتی و اقتصاد مبتنی بر دانش مشارکت فعال داشته باشد، از مزایای کامل آن بهره‌مند شود و آن‌ها را درک کند.»

APCICT برای تحریک مخاطب به پاسخ‌گویی سریع، دوره آموزشی توسعه به کمک فناوری اطلاعات و ارتباطات را مهیا کرده است. آکادمی الزامات فناوری اطلاعات و ارتباطات، برای مدیران ارشد دولتی در سال ۲۰۰۸ آغاز به کار کرد و مبتنی بر تقاضای بسیاری از کشورهای عضو، در حال حاضر ۱۰ سرفصل مجزا اما به‌هم مرتبط دارد که هدفش سهیم ساختن متخصصان و فراهم آوردن دانش لازم در کمک به طراحی و اجرای مؤثرتر نوآوری‌های فناوری اطلاعات و ارتباطات توسط سیاست‌گذاران است. پذیرش گسترده برنامه آکادمی در سراسر آسیا و اقیانوسیه گواهی بر پوشش لحظه‌ای و مرتبط مطالب این سرفصل‌ها است.

ESCAP از تلاش‌های در جریان APCICT در جهت به‌روزرسانی و انتشار سرفصل‌های آموزشی با کیفیت در دنیای در حال تغییر فناوری و بهره‌مندی ذی‌نفعان ملی و منطقه‌ای از دانش توسعه به کمک فناوری اطلاعات و ارتباطات استقبال می‌کند. با این وجود، ESCAP، از طریق APCICT به ترویج استفاده، سفارشی‌سازی و ترجمه سرفصل‌های آکادمی در کشورهای مختلف می‌پردازد. امیدوارم از طریق ارائه منظم کارگاه‌های ملی و منطقه‌ای برای کارمندان ارشد و مدیران میانی دولت، دانش لازم برای آگاهی بهتر از منافع فناوری اطلاعات و ارتباطات و اقدامات صریح به سمت برآوردن اهداف توسعه ملی و منطقه‌ای صورت گیرد.

Noeleen Heyzer
معاون دبیر کل سازمان ملل متحد و دبیر اجرایی ESCAP

مقدمه

در تلاش برای ایجاد پل روی شکاف‌های دیجیتالی، اهمیت توسعه منابع انسانی، ظرفیت سازمانی و استفاده از فناوری‌های اطلاعاتی و ارتباطی را نمی‌توان نادیده گرفت. این فناوری‌ها ابزارهای ساده‌ای هستند، اما وقتی مردم بدانند که چطور استفاده مؤثری از آن‌ها داشته باشند، به محرک‌های تغییر شکل‌دهنده‌ای تبدیل می‌شوند که به‌سرعت توسعه اقتصادی- اجتماعی می‌افزارند و تغییرات مثبتی ایجاد می‌کنند. با این چشم‌انداز، آکادمی الزامات فناوری اطلاعات و ارتباطات برای مدیران ارشد دولتی توسعه یافت.

آکادمی، مهم‌ترین برنامه APCICT به شمار می‌رود و برای تجهیز مقامات دولتی با دانش و مهارت‌ها، با هدف بهره‌برداری کامل ایشان از فناوری اطلاعات و ارتباطات برای توسعه اقتصادی و اجتماعی طراحی شده است. آکادمی از زمان شروع به کار رسمی‌اش در سال ۲۰۰۸ به هزاران فرد و صدها مؤسسه در سراسر منطقه آسیا و اقیانوسیه و فراتر از آن دست‌یافته است. آکادمی در بیش از ۲۰ کشور در منطقه آسیا و اقیانوسیه دایر شده است و در چارچوب‌های آموزشی منابع انسانی دولتی متعدد، پذیرفته شده است و همچنین در برنامه درسی دانشگاه‌ها و دانشکده‌های این منطقه نیز گنجانده شده است.

آکادمی تا حدی متأثر از به نتیجه محتوای جامع و دامنه هدفمند عناوین هشت سرفصل اول آن، و نیز توانایی پیکربندی سرفصل‌ها در تأمین محتوای محلی و پرداختن به مسائل توسعه اقتصادی- اجتماعی است. APCICT در سال ۲۰۱۱، در نتیجه تقاضای زیاد کشورهای آسیا و اقیانوسیه، با مشارکت شبکه شرکای خود دو سرفصل جدید آموزشی آکادمی طراحی کرد. این سرفصل‌ها برای افزایش ظرفیت استفاده از فناوری اطلاعات و ارتباطات برای مدیریت ریسک بلایا و کاهش تغییرات اقلیمی تعریف شدند.

سرفصل‌های جدید ۹، ۱۰ و ۱۱، همانند سرفصل‌های ۱ تا ۸ بر اساس رویکرد « We D.I.D It In Partnership» APCICT توسعه یافتند، اجرا و به‌صورت جامع و مشارکتی ارائه شدند و به‌طور نظام‌مند از گروه استثنایی و عظیم ذی‌نفعان توسعه استفاده کردند. کل آکادمی مبتنی بر این موارد بوده است: ارزیابی نیازهای منطقه آسیایی- اقیانوسیه‌ای بر اساس تحقیقات میدانی؛ مشاوره با مقامات دولتی، اعضای جامعه بین‌المللی توسعه و اساتید دانشگاه‌ها؛ پژوهش و تحلیل درباره نقاط قوت و ضعف مطالب آموزشی موجود؛ و فرآیند مرور همکاری که از راه کارگاه‌های منطقه‌ای و محلی مجموعه‌های APCICT انجام شده‌اند. این کارگاه‌ها فرصت‌های ارزشمندی برای تبادل تجربیات و دانش در میان کاربران آکادمی کشورهای مختلف فراهم ساختند. نتیجه آن، تدوین برنامه آموزشی آکادمی، با ۱۰

سرفصل جامع، پوشش عناوین مهم توسعه به کمک فناوری اطلاعات و ارتباطات و بیان بسیاری از صداها و تفاوت‌های ظرفیت بافت‌های منطقه بود.

رویکرد جمعی و فراگیر APCICT برای توسعه آکادمی، شبکه‌ای از شرکای قدرتمند را برای هماهنگی در ارائه آموزش توسعه به کمک فناوری اطلاعات و ارتباطات به مقامات دولتی، سیاست‌گذاران و ذی‌نفعان توسعه در کل منطقه آسیایی و اقیانوسیه و فراتر از آن، به وجود آورده است. در نتیجه همکاری نزدیک بین APCICT و مؤسسات آموزشی، آژانس‌های دولتی و سازمان‌های بین‌المللی و منطقه‌ای، چارچوب‌های آموزشی آکادمی در سطوح ملی و منطقه‌ای در کشورها و مناطق مختلف عرضه و پذیرفته می‌شوند. این اصل همچنان نیروی محرک باقی خواهد ماند، زیرا APCICT با شرکایش، برای به‌روزرسانی و بومی‌سازی مداوم مطالب آکادمی، توسعه سرفصل‌های جدید برای پرداختن به نیازهای مشخص و افزایش دسترسی مخاطبان جدید هدف به محتوای آکادمی از طریق رسانه‌های جدید و قابل‌دسترس‌تر کار می‌کند.

APCICT با تکمیل ارائه رودرروی برنامه آکادمی، پلت‌فرم آنلاین آموزش از راه‌دور Virtual Academy را توسعه داده است (http://e-learning.unapcict.org) که برای مطالعه شرکت‌کنندگان برمبنای سرعت خودشان طراحی می‌شود. Virtual Academy تضمین می‌کند که تمام سرفصل‌ها و مطالب همراه به‌سادگی دانلود، اشاعه، شخصی‌سازی و بومی‌سازی می‌شوند. هم‌چنین آکادمی روی DVD برای افرادی که محدودیت اتصال به اینترنت دارند قابل‌دسترس است.

APCICT برای افزایش دسترسی و ارتباط با محتوای محلی با همکاری شرکایش آکادمی را به زبان‌های انگلیسی، اندونزیایی، مغولی، میانماری، روسی، تاجیک و ویتنامی در دسترس قرار داده است و ترجمه سرفصل‌ها به زبان‌های دیگر را طرح‌ریزی می‌کند.

بدیهی است، توسعه و ارائه آکادمی بدون تعهد، ایثار و مشارکت فعال افراد و سازمان‌های مختلف ممکن نخواهد بود. از این فرصت استفاده می‌کنم تا از تلاش‌ها و دستاوردهای همکارانمان در وزارتخانه‌های دولتی، مؤسسات آموزشی و سازمان‌های ملی و منطقه‌ای که در کارگاه‌های آکادمی مشارکت داشته‌اند، تشکر و قدردانی کنم. آن‌ها نه تنها ورودی‌های ارزشمندی به محتوای سرفصل‌ها ارائه دادند، بلکه مهم‌تر، مدافعان آکادمی در کشورها و مناطق خود شدند و کمک کردند، آکادمی به مؤلفه مهم چارچوب‌های ملی و منطقه‌ای برای ظرفیت‌سازی فناوری اطلاعات و ارتباطات در تأمین آرمان‌های آتی توسعه اجتماعی- اقتصادی تبدیل شود.

من می‌خواهم بابت تلاش‌های بی‌دریغ بسیاری از شرکت‌کنندگان برجسته‌ای که سرفصل ۵ را ایجاد کردند و هم‌چنین نویسنده سرفصل؛ Ang Peng Hwa؛ صمیمانه قدردانی کنم. به‌علاوه می‌خواهم از بیش از ۷۵۰۰ شرکت‌کننده تشکر کنم که در بیش از ۸۰ کارگاه آکادمی در بیش از ۲۰ کشور و

هم‌چنین آموزش آنلاین شرکت کرده‌اند. بازخورد و بینش ارزشمند آن‌ها به ایجاد اطمینان از اینکه آکادمی تأثیری پایدار دارد، کمک کرده است.

امیدوارم آکادمی به کشورها کمک کند، شکاف‌های منابع انسانی فناوری اطلاعات و ارتباطات را کاهش دهند، موانع پذیرش فناوری اطلاعات و ارتباطات را از میان بردارند و کاربرد فناوری اطلاعات و ارتباطات در توسعه سریع اقتصادی- اجتماعی و دست‌یابی به اهداف توسعه هزاره را ارتقا بخشند.

Hyeun- Suk Rhee
مدیر UN-APCICT/ESCAP

درباره مجموعه سرفصل‌ها

در «عصر اطلاعات» امروزی، دسترسی آسان به اطلاعات، در حال تغییر روش زندگی، کار و بازی است. ویژگی «اقتصاد دیجیتال» یا «اقتصاد مبتنی بر دانش»، «اقتصاد شبکه‌ای» یا «اقتصاد نوین» انتقال از تولید کالا به خلق ایده‌ها است. این امر در نقش رشد با استفاده از فناوری‌های اطلاعاتی و ارتباطی در اقتصاد و در جامعه به‌عنوان کل تأکید دارد.

در نتیجه، دولت‌ها در سراسر جهان تمرکز فزاینده‌ای بر توسعه به کمک فناوری اطلاعات و ارتباطات دارند. از نظر دولت‌ها توسعه به کمک فناوری اطلاعات و ارتباطات، نه تنها درباره توسعه صنعت یا بخش فناوری اطلاعات و ارتباطات در اقتصاد است، بلکه استفاده از آن را برای ایجاد رشد اقتصادی و نیز سیاسی و اجتماعی در برمی‌گیرد.

با این وجود، یکی از مشکلاتی که دولت‌ها در تنظیم سیاست فناوری اطلاعات و ارتباطات با آن مواجه هستند، آن است که سیاست‌گذاران اغلب با فناوری‌هایی که برای توسعه ملی به کار می‌برند آشنا نیستند. از آنجایی که نمی‌توان چیزی را که درک نشده تنظیم کرد، بسیاری از سیاست‌گذاران شرمنده از سیاست‌گذاری فناوری اطلاعات و ارتباطات بوده‌اند، اما سیاست‌گذاری فناوری اطلاعات و ارتباطات از سوی متخصصان فناوری نیز اشتباه است، زیرا اغلب آن‌ها با تأثیرات سیاسی فناوری‌ها آشنایی ندارند.

آکادمی الزامات فناوری اطلاعات و ارتباطات برای مدیران ارشد دولتی، از سوی UN-APCICT/ESCAP برای افراد زیر توسعه‌یافته است:

۱- سیاست‌گذاران سطح دولت ملی و محلی که مسئول سیاست‌گذاری فناوری اطلاعات و ارتباطات هستند.
۲- مقامات دولتی مسئول توسعه و پیاده‌سازی کاربردهای مبتنی بر فناوری اطلاعات و ارتباطات.
۳- مدیران بخش دولتی جویای استفاده از ابزارهای فناوری اطلاعات و ارتباطات برای مدیریت پروژه.

هدف سری‌های سرفصل افزایش آشنایی با مسائل اساسی توسعه به کمک فناوری اطلاعات و ارتباطات از منظرهای سیاست و فناوری است. قصد آن توسعه دستورالعمل فنی فناوری اطلاعات و ارتباطات نیست، بلکه درک خوبی از توانایی فناوری دیجیتال کنونی است یا این‌که فناوری کجا در صدر قرار می‌گیرد و چه پیامدهای ضمنی برای سیاست‌گذاری به همراه دارد. عناوین سرفصل‌ها از طریق تحلیل نیازهای آموزشی و تحقیق میدانی در سایر مطالب آموزشی سراسر دنیا شناسایی شده‌اند.

سرفصل‌ها به‌صورتی طراحی شده‌اند که بتوانند برای خودخوانی یا منبع دوره و برنامه آموزشی استفاده شوند. آن‌ها مجزا و در عین حال با یکدیگر ارتباط دارند و تلاش شده است، هر سرفصل با درونمایه و مباحث سایر سرفصل‌های این سری ارتباط داشته باشد. هدف بلندمدت، منسجم ساختن دوره آموزشی سرفصل‌ها برای دریافت گواهی‌نامه است.

هر سرفصل با بیان اهداف و خروجی‌های آموزشی آغاز می‌شود و در مقابل خوانندگان می‌توانند پیشرفت خود را ارزیابی کنند. محتوای سرفصل به بخش‌هایی تقسیم می‌شود که شامل مطالعات موردی و تمرین‌هایی برای کمک به درک عمیق مفاهیم کلیدی هستند. خوانندگان می‌توانند تمرین‌ها را به‌صورت فردی یا گروهی انجام دهند. شکل‌ها و جداول برای نمایش جنبه‌های خاص بحث ارائه شده‌اند. فهرست مراجع و منابع آنلاین برای خوانندگان ارائه شده است تا منظرهای بیشتری به دست آورند.

استفاده از توسعه به کمک فناوری اطلاعات و ارتباطات، به‌قدری متنوع است که گاهی مطالعات موردی و مثال‌های سرفصل متناقض به نظر می‌رسند. این امر انتظار می‌رود و هیجان و چالش این رشته نوظهور به شمار می‌رود. امید است که تمام کشورها شناسایی پتانسیل فناوری‌های اطلاعاتی و ارتباطی را به‌عنوان ابزار توسعه آغاز کنند.

پشتیبانی سری سرفصل‌های آکادمی به‌صورت چاپی، پلت‌فرم آنلاین، آموزش از راه دور (APCICT Virtual Academy)، کلاس‌های درس مجازی از تدریس مربیان با فرمت ویدئویی و اسلایدهای نمایشی از سرفصل‌ها بهره می‌برند، (visit http://e-learning.unapcict.org را ببینید).

به‌علاوه، APCICT مرکز همکاری الکترونیکی را برای توسعه، به کمک (http://www.unapcict.org/ecohub) بسط داده است. سایت آنلاین مختص کارمندان و سیاست‌گذاران توسعه به کمک فناوری اطلاعات و ارتباطات برای بهبود تجربه آموزش و یادگیری آن‌هاست. این مرکز دسترسی به منابع دانش، جنبه‌های مختلف توسعه به کمک فناوری اطلاعات و ارتباطات، فضایی تعاملی برای تسهیم دانش و تجربیات و همکاری برای پیشرفت توسعه به کمک فناوری اطلاعات و ارتباطات را مهیا می‌سازد.

سرفصل ۵

اینترنت چالش‌های قابل‌توجهی برای سیاست عمومی و توسعه پایدار انسانی، هم در سطح بین‌المللی و هم در سطح ملی ایجاد می‌کند. از این رو، توسعه مداوم رویه‌ها و سیاست‌های بین‌المللی جهت نظارت[1] بر استفاده و بهره‌برداری از اینترنت ضروری است. با این وجود، هرچند منطقه آسیا و اقیانوسیه بیشترین سهم کاربران اینترنتی را در سطح جهان دارد، در فوروم‌ها[2] توسعه سیاست‌های مربوط به اینترنت کمتر نشان داده شده است. در مفهوم منطقه‌ای چندین مسئله و چالش ویژه مربوط به نظارت بر اینترنت[3] وجود دارد. برای این‌که نظارت بر اقتصادهای نوظهور در شبکه اطلاعات جهانی حرفی برای گفتن داشته باشند، نیاز به درک این مسائل دارند.

اهداف سرفصل

اهداف این سرفصل عبارتند از:

۱- تشریح توسعه مداوم رویه‌ها و سیاست‌های بین‌المللی که بر استفاده و کاربرد اینترنت نظارت می‌کند.

۲- مرور کلی مسائل و چالش‌های ویژه مربوط به نظارت بر اینترنت در مفهوم منطقه‌ای.

نتایج یادگیری

بعد از کار با این سرفصل، خوانندگان باید بتوانند:

۱- توسعه رویه‌ها و سیاست‌های بین‌المللی را برای نظارت بر استفاده و کاربرد اینترنت تشریح کنند.

۲- در مورد مسائل کلیدی نظارت بر اینترنت از دیدگاه کشورهای در حال توسعه بحث کنند.

۳- گام‌های اولیه برای نظارت بهتر بر اینترنت را در کشورهای خود طرح‌ریزی کنند.

1- Govern
2- Forums
3- Internet Governance

اختصارات

ACPA	Anti-Cybersquatting Consumer Protection Act
ACTA	Anti-Counterfeiting Trade Agreement
APCICT	Asian and Pacific Training Centre for Information and Communication Technology for Development
ccTLD	Country Code Top-Level Domain
CoE	Council of Europe
CSC	Common Services Centre (India)
DEC	Digital Equipment Corporation
DNS	Domain Name System
ESCAP	Economic and Social Commission for Asia and the Pacific (UN)
EU	European Union
FOSS	Free and Open Source Software
GAC	Government Advisory Committee
GNSO	Generic Names Supporting Organization
GPS	Global Positioning System
gTLD	Generic Top-Level Domain
ICANN	Internet Corporation for Assigned Names and Numbers
ICPEN	International Consumer Protection and Enforcement Network
ICRA	Internet Content Rating Association
ICT	Information and Communication Technology
ICTD	Information and Communication Technology for Development
IDN	Internationalized Domain Name
IP	Internet Protocol
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
ITU	International Telecommunication Union
MDG	Millennium Development Goal
OECD	Organisation for Economic Co-operation and Development
PPP	Public-Private Partnership
RIAA	Recording Industry Association of America
RIR	Regional Internet Registry
TCP/IP	Transmission Control Protocol/Internet Protocol
TLD	Top-Level Domain
UDRP	Uniform Dispute Resolution Process
UK	United Kingdom
UN	United Nations
USA	United States of America
WGIG	Working Group on Internet Governance
WIPO	World Intellectual Property Organization
WSIS	World Summit on the Information Society

لیست آیکن‌ها


مطالعه موردی


پرسش‌هایی برای تفکر


فعالیت


خودآزمایی

فصل اول

مسئله و گستره نظارت بر اینترنت

هدف این بخش ارائه تاریخچه مختصری از مفهوم نظارت بر اینترنت و طرح خلاصه‌ای از گستره نظارت بر اینترنت است.

۱-۱ مقدمه

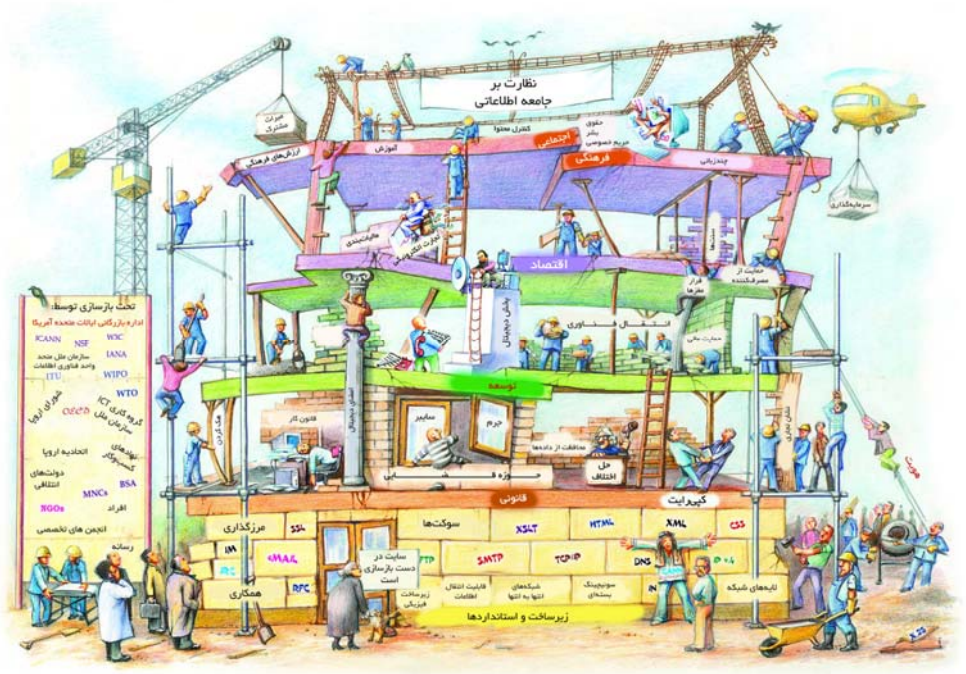
اغلب فرض بر این است که وسیله ارتباطی جدید به نام اینترنت قابل‌کنترل نیست. کاربران اولیه آن اغلب با صدای بلند می‌گویند که اینترنت اختراعی است که برای نجات یک حمله هسته‌ای، محاصره کامل با مسیریابی از اطراف، از بین بردن مرزهای چندگانه بین‌المللی و بنابراین ضد سانسور[۱] است. ضد سانسور به این معناست که اگرچه اداره محتوای اینترنت غیرممکن نیست ولی دشوار است و بنابراین کنترل کاربران آن نیز مسئله است.[۱]

اکنون بیش از ۱۰ سال بعد از عمومی شدن دسترسی به اینترنت، می‌دانیم که این تصورات درباره اینترنت افسانه هستند و اینترنت قابل‌کنترل است. در حقیقت، این کشورهای توسعه یافته‌تر هستند که مقررات[۲] بیشتری برای اینترنت دارند، در حالی که کشورهای کمتر توسعه یافته دارای مقررات کم یا هیچ مقرراتی برای نظارت بر اینترنت ندارند. کمبود قوانین ممکن است منجر به تبدیل این کشورها به پناهگاهی برای افرادی شود که با استفاده از اینترنت کارهای خلافی مانند هرزنامه[۳] و اسکم[۴] انجام می‌دهند.

این کمیت قوانین و مقررات نیست که استفاده از اینترنت را کاهش می‌دهد. اگر چنین بود، ایالات متحده آمریکا (USA) بیشترین کاهش را در استفاده از اینترنت داشت و کشوری مانند لائوس که هنوز در حال کشمکش با مسائل زیرساختی است؛ در اینترنت پیشرفت می‌کرد. آنچه اهمیت دارد این است که قوانین ناظر بر اینترنت باید بر اساس درک کامل مسائل قانونی و فنی و از طریق مشارکت

1- Censor-Proof
2- Regulations
3- Spam
4- Scams

بین‌المللی ایجاد شوند. هدف این سرفصل شرح این مسائل است و نشان می‌دهد که چگونه مشارکت بین‌المللی در نظارت بر اینترنت قابل‌دستیابی است.



شکل ۱-۱ نظارت بر جامعه اطلاعاتی: مرور

منبع: DiploFoundation, http://textus.diplomacy.edu/textusbin/env/scripts/Pool/GetBin.asp?IDPool=1190.

۱-۲ سابقه تاریخی و فنی اینترنت

توسعه تاریخی و فنی

اینترنت برای ایجاد یک شبکه ارتباطی که از یک حمله هسته‌ای جان به در ببرد، ابداع نشده است، بلکه هدف آن این است که به فیزیک‌دانان امکان به اشتراک‌گذاری کامپیوترها را برای حل مسائل پیچیده محاسباتی بدهد. کامپیوترها قبلاً تجهیزاتی بزرگ و گران و در مکان‌های پراکنده گسترده شده بودند.[۲] در شیوه اتصال کامپیوترها از یک پروتکل[1] ابداع شده در دهه ۱۹۶۰ استفاده

1- Protocol

شده است که به فناوری شبکه وابسته نیست و این یک درک متقابل دارد، زیرا ممکن است چنین تصور شود که برای ارسال پیام از یک مکان به مکانی دیگر باید از فناوری و تجهیزات خوب استفاده شود. اما این پروتکل، ارسال تراکنش‌ها و پیام‌های کامپیوتری را به‌صورت بسته‌بندی امکان‌پذیر و سپس آن‌ها را در سمت گیرنده اصلاح می‌کند. اگر پیام صحیح یا واضح دریافت نشود، دوباره فرستاده می‌شود. چنین روشی برای انتقال، یعنی استفاده از شبکه یا کانال ارتباطی[۱] نیاز به «هوشمندی»[۲] ندارد. تمام چیزی که نیاز است مسیریاب‌ها[۳] برای تعیین مسیر پیام‌ها است که با آن پیام‌ها راه خود را از طریق «شبکه احمق»[۴] پیدا می‌کنند. این «پروتکل ارتباط شبکه‌ای از طریق اینترنت»[۵] در کمک به عبور پیام‌ها از شبکه‌های مختلف، برتر از پروتکلی است که برای تلفن استفاده می‌شد.

برتری پروتکل ارتباط شبکه‌ای از طریق اینترنت از دهه؛۱۹۷۰ هنگامی‌که شرکت‌های تلفن شروع به هوشمند ساختن شبکه‌های خود کردند؛ مشخص شد.[۳] اگرچه اتحادیه مخابرات بین‌المللی (ITU)[۶] که یک آژانس سازمان ملل برای هماهنگی مخابرات جهانی بود؛ تعدادی پروتکل و استاندارد ارائه داد، اختلاف بین چشم‌اندازها منجر به برخوردی شد که در نهایت به نفع پروتکل ارتباط شبکه‌ای از طریق اینترنت در برابر پروتکل شرکت‌های تلفنی شد.

تاریخچه نظارت بر اینترنت[۴]

باید به یاد داشته باشیم که پروتکل‌ها و استانداردها در دنیای فناوری بسیار اهمیت دارند، زیرا هرکس که این موارد را کنترل می‌کند اگر نتواند مسیر فناوری را کنترل کند، می‌تواند آن را تحمیل کند. در حال حاضر پروتکلی که برای اتصال شبکه‌های مختلف در اینترنت به کار می‌رود، پروتکل کنترل انتقال/پروتکل اینترنت (TCP/IP)[۷] نامیده می‌شود. این پروتکل در سال ۱۹۷۴ توسط وینتون جی. سرف و باب کوهن[۸] ابداع شد و برای کارکرد شبکه به‌قدری حیاتی بود که هر شبکه‌ای که از TCP/IP استفاده می‌کرد به‌عنوان اینترنت شناخته می‌شد.

در جهت اهداف این سرفصل، قابل‌توجه‌ترین اصل پروتکل این است که کنترل مستقیمی روی ارتباطات اینترنتی وجود نداشت؛ فقط باید آدرس ارتباطات کنترل می‌شد. مسئله آدرس یعنی این‌که باید فردی وجود داشته باشد تا از عدم برخورد آدرس‌ها اطمینان داشته باشد. در سیستم آدرس‌دهی جهانی برای طراحی شبکه‌ها از اعداد استفاده می‌شود. برخی از افراد یا عوامل باید اطمینان داشته

1- Pipe
2- Intelligence
3- Routers
4- Stupid Network
5- Internetworking Protocol
6- International Telecommunication Union
7- Transmission Control Protocol/Internet Protocol
8- Vinton G. Cerf and Bob Kahn

باشند که هیچ دو آدرسی از اعداد یکسان استفاده نمی‌کنند و باید یک دایرکتوری مرکزی برای حذف چنین تعارضاتی وجود داشته باشد. چنین بود که جان پوستال[۱] که تمام مدارک خود را از دانشگاه کالیفرنیا در لس‌آنجلس گرفت، بعداً شهر را به مقصد دانشگاه کالیفرنیای جنوبی ترک کرد تا مدیر مؤسسه علوم اطلاعاتی[۲] شود و همان‌طور که اکونومیست[۳] او را نام‌گذاری کرد؛ «خدای اینترنت»[۴] شد. او چنین تعارضاتی را حل می‌کرد تا اینترنت به رشد خود ادامه دهد.

با رشد تعداد شبکه‌ها، به خاطر سپردن اعداد آن‌ها مسئله می‌شد. بنابراین در سال ۱۹۸۳، پوستال و پاول موکاپتریس[۵] پیشنهاد دادند به‌جای اعداد از نام استفاده شود. به‌عنوان مثال، در موتور جست‌وجو به‌جای تایپ 64.233.161.18 باید google.com تایپ می‌شد. این کار معادل دادن نام‌ها به یک سیستم شماره‌گذاری تلفنی[۶] بود. بنابراین سیستم نام حوزه (DNS)[۷] به وجود آمد.

سیستم نام حوزه مسائل قانونی خاص خود را نیز دارد. این مسئله در بخش بعدی بحث خواهد شد. فعلاً درک DNS برای درک مسئله اهمیت دارد.[۵]

سیستم نام حوزه یک سیستم سلسله مراتبی است که از ساختار «درختی»[۸] برای سازمان‌دهی اطلاعات شبکه‌ها و کامپیوترها استفاده می‌کند. این سیستم شبیه آدرس پستی است که آدرس خیابان در ابتدا و نام کشور در انتهاست، بنابراین نام حوزه سطح بالا (LTD)[۹] در انتها و آدرس ویژه شبکه در ابتدا قرار می‌گیرد. بنابراین هنگامی‌که کامپیوتر در جست‌وجوی یک آدرس اینترنتی است از راست به چپ و نام هر سرور را از سمت چپ آن جست‌وجو می‌کند.

هنگامی‌که اولین بار در ژانویه ۱۹۸۵ این سیستم اجرا شد، ۶ حوزه سطح بالا وجود داشت:

COM: برای سازمان‌های تجاری[۱۰]

EDU: برای مؤسسات آموزشی[۱۱]

NET: برای ارائه‌دهندگان شبکه[۱۲]

ORG: برای سازمان‌های غیرانتفاعی[۱۳]

MIL: برای ارتش ایالات متحده[۱۴]

1- Jon Postal
2- Information Sciences Institute
3- The Economist
4- God of the Internet
5- Postal and Paul Mockapetris
6-Telephone Numbering System
7- Domain Name System
8- Tree-Like Structure
9- Top Level Domain
10- Commercial Organizations
11- Educational Institutions
12- Network Providers
13- Non-Profit Organizations
14- US Military

GOV: برای دولت ایالات متحده[۶]

پس از آن تعداد زیادی از حوزه‌های عمومی سطح بالا (gTLDs)[۱] اضافه شدند.[۷] شاید مهم‌ترین هدف کنونی ما ایجاد حوزه‌های کد کشوری سطح بالا (ccTLDs)[۲] است. این کدها به یکدیگر شباهت دارند، اما برای کدهای کشوری دو حرفی ISO 3166-1 alpha-2 برای کشورها و قلمروهای وابسته که در تجارت بین‌الملل[۳] استفاده می‌شوند؛ یکسان نیستند.[۸] ایالات متحده آمریکا نیز حوزه کد کشوری سطح بالای دو حرفی دارد. اما به دلیل تسلط تاریخی و مزیت پیشگامی[۴] آن، یک حوزه عمومی سطح بالا بدون کد کشوری؛ بخصوص COM؛ از ایالات متحده یا جایی دیگر می‌گیرد تا وسعت گسترده‌تری در جهان داشته باشد.

قابلیت دسترسی حوزه‌های کد کشوری سطح بالا به این معنی است که دولت‌ها حق بیشتری در تصمیم‌گیری در مورد نام‌های حوزه دارند. بنابراین مثلاً در مورد yahoo.fr، مدیر سیستم نام حوزه در فرانسه تصمیم‌گیرنده است. به همین دلیل در نمونه مشهور یک دادگاه فرانسوی این تصمیم گرفته شد که Yahoo نمی‌تواند در وب‌سایت خود که مخاطبان فرانسوی را هدف قرار می‌دهد؛ خاطرات نازی‌ها را بفروشد. دادگاه فرانسوی می‌توانست مداخله و چنین تصمیمی را اعمال کند زیرا نام حوزه- yahoo.fr- در فرانسه ثبت شده بود. سپس Yahoo نام وب‌سایت خود را برای کاربران فرانسوی زبان به fr.yahoo.com تغییر داد. اگر به‌عنوان یک آدرس خوانده شود، آدرس جدید وب‌سایت در Yahoo و سروری که برچسب FR روی آن خورده است، در فضای حوزه COM است. آدرس جدید به این معنی است که Yahoo می‌تواند قانون فرانسه را به مبارزه دعوت کند، اگرچه به نظر می‌رسد که هیچ دلیل تجاری برای چنین کاری وجود ندارد. در حقیقت، Yahoo نام کلیه سایت‌های خارجی خود را تغییر داد. به همین دلیل آدرس‌ها به COM منتهی می‌شوند.

از اواسط دهه ۱۹۹۰، درخواست‌هایی برای معرفی حوزه‌های عمومی سطح بالا وجود داشت. برخی حوزه‌های عمومی سطح بالای ویژه‌تر را می‌خواستند؛ در حالی که برخی دیگر در اداره یک حوزه عمومی سطح بالا یک فرصت مالی می‌دیدند. برای بیش از یک قرن، کمتر از ۲۰ حوزه عمومی سطح بالا ایجاد شد. در نهایت، در ژوئن ۲۰۱۱ در سنگاپور، شرکت اینترنتی اسامی و اعداد اختصاص یافته (ICANN)[۵] با اجرای پیشنهاد باز کردن کامل برنامه‌های کاربردی حوزه عمومی سطح بالا؛ به‌صورت نقطه-هرچه[۶] موافقت کرد. یعنی حوزه‌های عمومی سطح بالا می‌توانند برای نام‌های تجاری[۱]، شهرها و نام‌ها استفاده شوند. رأی‌گیری بدون منازعه نبود.

1- Generic TLDs
2- Country-Code TLDs
3- International Commerce
4- First-mover Advantage
5- Internet Corporation for Assigned Names and Numbers
6- Dot-Anything

یک نکته اصلی در منازعات این بود که در کنار سپرده‌گذاری ۵,۰۰۰ دلاری آمریکا، هزینه ارزیابی[۲] ۱۸۰,۰۰۰ دلاری نیز باید به‌عنوان بخشی از برنامه کاربردی برای اجرای حوزه عمومی سطح بالای جدید در نظر گرفته می‌شد. برخی احساس می‌کردند که این هزینه ممکن است مانعی برای برنامه‌های کاربردی در کشورهای در حال توسعه باشد. هم‌چنین این هزینه شامل حال افرادی که زودتر حوزه‌های عمومی سطح بالا را به دست آورنده بودند، نمی‌شد.[۹] کمیته مشاور دولت (GAC)[۱۰] در ICANN در اطلاعیه رسمی[۳] در می ۲۰۱۱ توضیح داد که هزینه‌ها کاهش داده می‌شوند و کشورهای در حال توسعه و داوطلبان نیازمند به مدت ۳ سال از هزینه ۲۵,۰۰۰ دلاری برای برنامه‌های کاربردی معاف هستند.[۱۱]

ICANN چهار مسئله کلیدی[۴] مربوط به معرفی حوزه‌های عمومی سطح بالا را مشخص می‌کند: (۱) محافظت از نام تجاری[۵]؛ (۲) پتانسیل هدایت شرورانه؛ (۳) مقیاس‌بندی منطقه‌ای ریشه[۶]/ثبات و امنیت و (۴) تقاضای حوزه سطح بالا و تحلیل اقتصادی.[۱۲]

هدف محافظت از نام تجاری این است که شرکت‌ها احساس می‌کنند باید نام شرکت‌هایشان را با حوزه سطح بالا ثبت کنند. با قانون «هرکس زودتر بیاید، اول نوبت اوست»[۷]، اگر نام تجاری خود را زود ثبت نکنند، ممکن است از بین برود. با این وجود، ثبت هزینه‌هایی را در بردارد. از زمان آن رأی انجمن‌های کسب‌وکار[۸] در هر دو طرف آتلانتیک از این پیشنهاد انتقاد کرده‌اند.[۱۳]

افرادی که رفتار شرورانه دارند، ممکن است به‌عنوان افرادی وارد اینترنت شوند که در اداره یک حوزه عمومی سطح بالا تازه واردند و ممکن است منابع مالی یا ظرفیت فنی برای محافظت از حوزه‌های خود در برابر حمله را نداشته باشند. بنابراین ثبات و امنیت حوزه سطح بالا ممکن است در معرض خطر قرار گیرد.[۱۴]

در اقتصاد، مسئله اصلی این است که آیا باید بین دفتر ثبت[۹] که حوزه سطح بالا را اداره می‌کند و ثبت‌کنندگان[۱۰] که نام‌های حوزه را می‌فروشند؛ تفکیک وجود داشته باشد یا خیر. ثبت حوزه عمومی جدید سطح بالا که توسط برخی افراد مورد بحث قرار می‌گیرد؛ ممکن است برای آن‌ها آن‌قدر منافع ایجاد نکند تا در مراحل اولیه خاص بمانند. هم‌چنین ثبت‌کنندگان ممکن است برای کار با یک حوزه

1- Brands
2- Evaluation Fee
3- Communiqué
4- Overarching Issues
5- Trademark
6- Root Zone
7- First-Come-First Served
8- Business Associations
9- Registry
10- Registrar

عمومی جدید سطح بالا در مقایسه با یک حوزه باسابقه انگیزه نداشته باشند، زیرا حوزه جدید نیاز به بازاریابی بیشتر خواهد داشت. بنابراین، اجازه به دفتر ثبت برای بازاریابی نیز؛ بخصوص یکپارچه‌سازی عمودی[1] کارکرد ثبت‌کننده؛ کسب‌وکار را بادوام‌تر خواهد کرد.

به عبارت دیگر، یکپارچه‌سازی عمودی به این معنی است که دفاتر ثبت باسابقه؛ مانند com.، net. و org.؛ نیز می‌توانند نام‌های حوزه را مستقیم بفروشند. این مسئله تمرکز بازار[2] و قدرت تجارت متصدیان را در صنعت نام حوزه افزایش خواهد داد.

ICANN با استفاده از دو مطالعه به این نتیجه رسید که یکپارچه‌سازی عمودی ممنوع نمی‌شود ولی قوانینی برای کنترل این یکپارچگی ایجاد می‌شوند.[۱۵] با این وجود، کمیسیون اروپا و اداره دادگستری ایالات متحده نامه‌هایی را به ICANN برای «تجدیدنظر»[۱۶] و «بررسی بیشتر»[۱۷] ارسال کردند. بنابراین یکپارچگی عمودی بین دفاتر ثبت و ثبت‌کنندگان در حال حاضر راکد است.

ضمناً، کمیته مشاور دولت نگرانی‌هایی درباره چگونگی مشارکت چشم‌اندازهای خود در دستورالعمل‌های شکل‌گیری حوزه‌های عمومی جدید سطح بالا دارد. در مارس ۲۰۰۷، این کمیته «اصول GAC درباره حوزه‌های عمومی جدید سطح بالا» را ارائه داد که علاوه بر موارد دیگر نشان می‌دهد که حوزه‌های عمومی جدید سطح بالا باید حساسیت‌های ملی، فرهنگی، جغرافیایی و مذهبی را در نظر بگیرند.[۱۸] این «استاندارد نظم عمومی و اخلاقی»[3]؛ همان‌طور که شناخته شده است؛ توسط اعضای جامعه مدنی[4] و برخی از اعضای GAC مورد انتقاد قرار گرفت. در یک یادداشت توصیفی در نوامبر ۲۰۰۸، ICANN اظهار داشت که این استانداردهای نظم عمومی و اخلاقی به سه حوزه محدود می‌شود:

- ✓ تشویق به اعمال خشن خلاف قانون
- ✓ تشویق یا ترویج تبعیض بر اساس نژاد، رنگ، جنسیت، قوم، مذهب یا منطقه ملی و
- ✓ تشویق یا ترویج هرزه‌نگاری یا هرگونه سوءاستفاده جنسی دیگر از کودکان.[۱۹]

اما GAC تناسب اصطلاح «نظم عمومی و اخلاقی» را در مارس ۲۰۱۱ مورد بررسی قرار داد.[۲۰] ICANN در نوامبر ۲۰۱۰ یک یادداشت توضیحی دیگر ارائه داد که معنی ضمنی آن را توصیف می‌کرد و هم‌چنین عنوان موضوع را به اعتراض «منافع عمومی محدود»[5] تغییر داد.[۲۱] با این وجود، رویه اعتراض نیاز به پرداخت هزینه توسط دولت‌ها دارد و همان‌طور که در عنوان اصلی اعتراض تعریف شد، آنچه دولت می‌تواند به آن اعتراض کند محدودیت دارد.[۲۲] بنابراین در آوریل ۲۰۱۱،

1- Vertical Integration
2- Market Concentration
3- Morality and Public Order Standard
4- Civil Society
5- Limited Public Interest

ICANN با یک یادداشت توضیحی دیگر ادامه داد، در این زمان اصطلاح «منافع عمومی محدود» کلاً حذف شد و با «اعتراضات دولت و GAC؛ مدیریت رشته‌های حساس؛ هشدار اولیه»[1] جایگزین شد. ممکن است دولت‌ها در حال حاضر به هر موضوعی بدون اجبار به موافقت با رویه اعتراض کنند که در این صورت نیاز به پرداخت هیچ هزینه‌ای نیست.[۲۳] با توجه به تاریخچه فرآیند اعتراض به نظر می‌رسد که این فرآیند همچنان ادامه دارد.

موضوع دیگری که هنوز ادامه دارد، تنظیم دقیق قوانین مربوط به نام‌های حوزه بین‌المللی (IDNs)[2] است. این قوانین؛ در تئوری؛ بهترین روش در جامعه غیر انگلیسی برای دسترسی به اینترنت هستند. با نام حوزه به زبان بومی، کاربران تجربه کار با اینترنت در منزل را به دست می‌آورند. بعد از پیشنهاد نام حوزه بین‌المللی به نظر می‌رسید که قابلیت اجرای فنی را در اواخر دهه ۱۹۹۰ داشته باشد. اما در می ۲۰۱۰ بود که حوزه کد کشوری سطح بالای نام حوزه بین‌المللی (IDN ccTLD) در منطقه ریشه راه‌اندازی شد.[۲۴] قبل از آن برخی از کشورها بخصوص چین، نام‌های حوزه را با کاراکترهای چینی اما فقط از طریق دفتر ثبت CN. خود می‌فروختند.

در کتاب راهنمای حوزه عمومی سطح بالا که توسط ICANN برای داوطلبین ارائه شد، نام حوزه بین‌المللی به‌عنوان یک نوع حوزه عمومی سطح بالا معرفی شد.[۲۵] در عرصه نام حوزه بین‌المللی این احساس وجود دارد که عدم تجانس در محیط می‌تواند باعث بسیاری از مسائل شود.[۲۶] نگرانی زیادی در مورد نام‌های «به شدت شبیه»[3] وجود دارد که به شاکیان اجازه می‌دهد که از ثبت‌نام‌ها جلوگیری کنند. یک کارگروه نام حوزه بین‌المللی در سازمان پشتیبانی از اسامی عمومی (GNSO)[4] در مارس ۲۰۰۷ گزارش داد که از محدود کردن نام‌هایی که از لحاظ بصری یا حروف‌چینی «به شدت شبیه» بودند پشتیبانی می‌شود.[۲۷] چنین قانونی برای جلوگیری از آنچه به‌عنوان حمله شباهت املایی[5] در نام حوزه بین‌المللی شناخته می‌شود و در آن یک زبان دوم به زبان اول ملحق می‌شود، ضروری است.[۲۸] به‌عنوان مثال در یک نمونه که در ویکی‌پدیا آورده شده است، از C سیریلیک[6] برای جایگزینی C لاتین در Citibank.com استفاده می‌شود. از آنجایی که رویکرد حوزه عمومی سطح بالا یک رویکرد نقطه-هرچه است، چنین تلفیق زبانی مجاز شده است.

1- Early Warning
2- Internationalized Domain Names
3- Confusingly Similar
4- Generic Names Supporting Organization
5- Homograph Attack

۶- خط سیریلیک یک خط الفبایی است که در امپراتوری مجارستان اول ایجاد شد. این خط اساس الفبای مورد استفاده در زبان‌های مختلف؛ به ویژه آن‌هایی که از منشأ اسلاوی هستند و زبان‌های غیراسلاوی تأثیر گرفته از روسی، چه در گذشته و چه امروزه؛ است. خط سیریلیک از خط یونان باستان با حروف بزرگ گرفته شده است (مترجم).

مسئله دیگر این است که کتاب راهنمای داوطلب در حوزه عمومی سطح بالا در 2.2.1.1.3 می‌گوید که «به‌هم‌ریختگی بر اساس هر نوع شباهت (شامل بصری، سمعی یا معنایی) ممکن است مورد انتقاد یک معترض قرار گیرد».[۲۹] برخی زبان‌ها مانند چینی یا هندی، آواهایی دارند که به کتاب راهنمای ثبت‌کننده امکان خواهد داد ثبت‌کننده‌های دیگر با آواهای مشابه در نام حوزه را مسدود کند.

در اواخر سال ۲۰۱۱، هر دو مسئله کاملاً حل شدند.

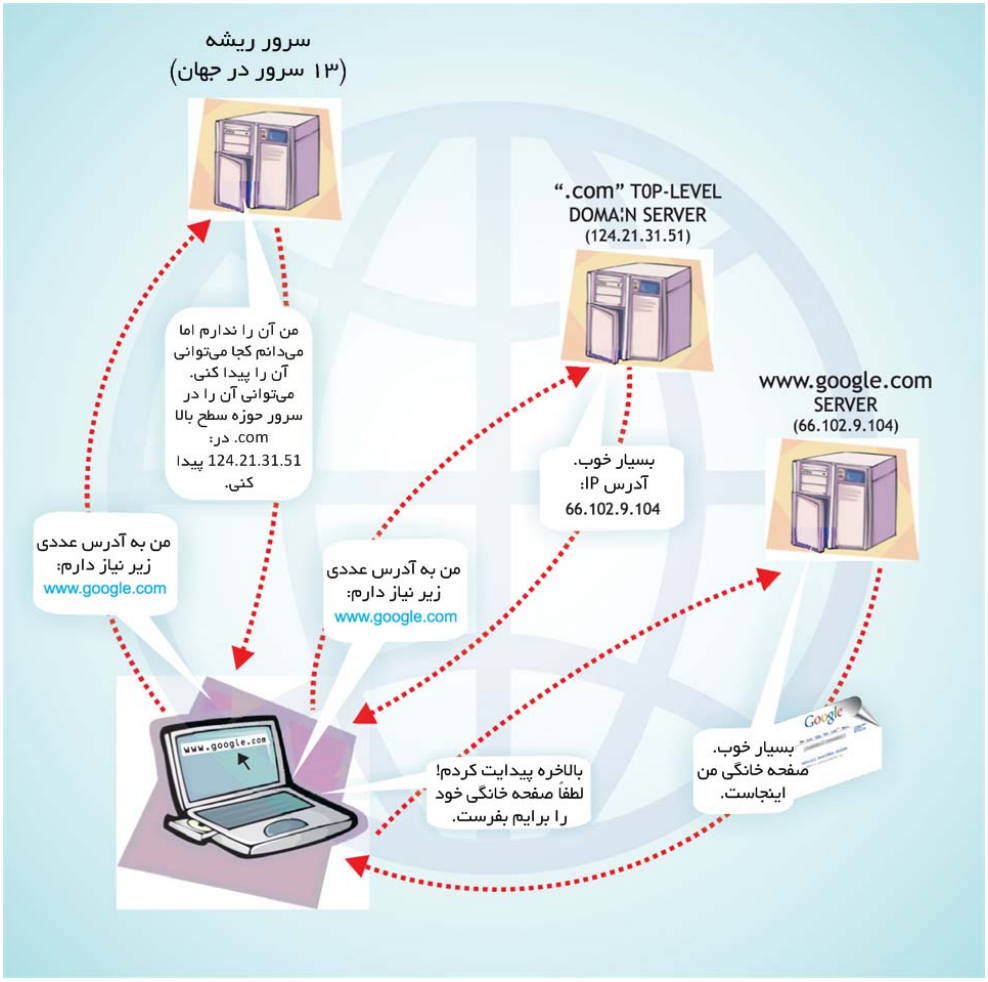
یک مسئله فنی‌تر مورد بحث دیگر سرور ریشه[۱] است. هنگامی‌که یک کامپیوتر به دنبال یک آدرس می‌گردد، از راست به چپ شروع به جست‌وجو می‌کند. هنگامی‌که حوزه عمومی سطح بالا در سمت راست یک آدرس وب قرار دارد، اولین جایی که کامپیوتر باید جست‌وجو کند منتهی‌الیه سمت راست است. بنابراین برای www.google.com کامپیوتر باید به دنبال com. بگردد. در اینجا کد جدید سیستم نام حوزه یک کد ضمنی «درج»[۲] کرده است: کلیه نام‌های حوزه اینترنتی در حقیقت با یک نقطه یا یک وقفه کامل (".") که به سروری به نام سرور ریشه مربوط می‌شود، منتهی می‌شوند. ۱۳ سازمان ریشه‌ای[۳] به نام اپراتور سرور ریشه به وجود آمده است تا سرورهایی با برچسب‌های A تا M را اداره کنند. توابع سرور A به‌عنوان سرور اصلی[۴]، با سرورهای B تا M روزانه چندین مرتبه با یکدیگر ارتباط دارند تا اطلاعات در جریان باشد. در عمل بسیاری از اطلاعات در سرورهای دیگر در نقاط مختلف جهان برای افزونگی[۵] ذخیره می‌شوند تا ترافیک اینترنت را به حداقل برسانند و سرعت دسترسی را افزایش دهند. این محدوده کامل ناحیه ریشه[۶] نام دارد.[۳۰] از آنجایی که منطقه ریشه در اداره اینترنت حیاتی است، حتی یک سرور به نام سرور مخفی[۷] وجود دارد که از چشم هکرها پوشیده است. سرورهای اصلی و مخفی هر دو در ایالات متحده آمریکا واقع شده‌اند.

در اینجا این سؤال پیش می‌آید که اگر کشوری در حال جنگ با ایالات متحده آمریکا باشد، چه اتفاقی برای اینترنت آن کشور می‌افتد. به‌عنوان مثال، آیا دولت ایالات متحده می‌تواند آن کشور را از فایل منطقه ریشه حذف کند تا اینترنت قطع شود یا خیر.

قبل از جنگ عراق، نام حوزه IQ از اینترنت حذف شد. حوزه IQ توسط هیچ‌یک از طرفداران صدام حسین اداره نمی‌شد، بلکه عرب‌های فلسطینی در تگزاس آن را مدیریت می‌کردند. اپراتورهای نام حوزه، برادران الاشی[۸] و شرکای کاری آن‌ها در سال ۲۰۰۲ به علت اتهام صادرات غیرقانونی قطعات کامپیوتر به لیبی و سوریه دستگیر شدند. در همین زمان سیستم نام حوزه IQ دقیقاً قبل از جنگ قطع

1- Root Server
2- Insert
3- Root Organization
4- Master Server
5 Redundancy
6- Root Zone
7- Hidden Server
8- Elashi

شد. در ۲۸ ژولای ۲۰۰۵ یعنی زمان تکمیل گزارش، کارگروه نظارت بر اینترنت سازمان ملل (WGIG)[1] و قبل از ترجمه آن به زبان‌های رسمی سازمان ملل، نام حوزه IQ به دولت عراق داده شد، زیرا در آن زمان فقط دولت عراق پایدار و فعال بود.



شکل ۲-۱ قرار دادن یک وب‌سایت روی اینترنت

منبع: DiploFoundation، http://textus.diplomacy.edu/textusbin/env/scripts/Pool/GetBin.asp?IDPool=1175.

1- UN-appointed Working Group on Internet Governance

کنترل منطقه ریشه به‌عنوان یک مسئله کلیدی در نظارت بر اینترنت دیده می‌شود. با این وجود نگرانی‌های مرتبط دیگری نیز وجود دارد. برخی از کشورها درباره مسئله توزیع آدرس‌های پروتکل اینترنت (IP) نگران بوده‌اند. به علت توسعه اینترنت به یک روش تصادفی و غیرقابل‌پیش‌بینی، برخی از دانشگاه‌های ایالات متحده آدرس‌های IP بیشتری نسبت به کشورهای دیگر دارند. این مسئله فقط پایه‌ای برای توزیع آدرس‌های IP به کار نمی‌رود، بلکه تعیین می‌کند که آیا آدرس‌های IP تمام می‌شوند یا خیر. تحت سیستم پروتکل اینترنت نسخه ۴ (IPv4)[1]، 4,294,967,296 آدرس یکتای IP وجود دارد. از آنجایی که جمعیت جهانی بسیار بیشتر از این رقم است، امکان تمام شدن آدرس‌های IP وجود دارد. این موضوع تا حدودی با استفاده مؤثرتر از سیستم آدرس IP و معرفی نسخه ۶ پروتکل اینترنت با 340, 282, 366, 920, 938, 463, 463, 374, 607, 431, 768, 211, 456 (340 تریلیون تریلیون تریلیون) آدرس یکتای IP، حل شد.[۳۱]

مسئله نظارت بر اینترنت در سال ۲۰۰۳ در مجمع جهانی در مورد جامعه اطلاعاتی (WSIS) مطرح شد. در حالی که بسیاری از کشورها قصد داشتند مسئله نظارت بر اینترنت را بررسی کنند، اما ایالات متحده آمریکا معتقد بود که ظرفیت کافی بخصوص در کشورهای در حال توسعه برای بررسی مسئله وجود ندارد. بنابراین، تصمیم بر این شد که یک کارگروه توسط دبیر کل سازمان ملل برای گزارش‌دهی موضوع منصوب شود. بیانیه اصول مجمع جهانی در مورد جامعه اطلاعاتی بیان می‌کند که:

۵۰. مسائل بین‌المللی نظارت بر اینترنت باید به یک روش هماهنگ بررسی شوند. ما از دبیر کل سازمان ملل متحد می‌خواهیم تا یک کارگروه طی یک فرآیند باز و فراگیر برای نظارت بر اینترنت راه‌اندازی کند تا سازوکاری برای مشارکت همه‌جانبه و فعالانه دولت‌ها، بخش خصوصی و جامعه نظامی هم در کشورهای توسعه یافته و هم در حال توسعه شامل فوروم‌ها و سازمان‌های بین‌المللی و بین دولتی مربوطه ایجاد شود تا پیشنهادهای عملی برای نظارت بر اینترنت در سال ۲۰۰۵ ارائه دهد.[۳۲]

همان‌طور که این کمیته می‌گوید کارگروه نظارت بر اینترنت شامل ۴۰ مأمور کشف حقیقت است تا تعیین کنند که نظارت بر اینترنت دقیقاً درباره چیست، چه نتایجی در بر دارد و چه کسی باید چه کاری را انجام دهد. در ادامه، گزارش کارگروه نظارت بر اینترنت را خواهیم آورد.

پرسش‌هایی برای تفکر

نظارت بر اینترنت برای کشور شما چقدر اهمیت دارد؟

1- Internet Protocol Version 4

خودآزمایی

۱- چرا اینترنت ابداع شد؟
۲- اغلب گفته می‌شود که اینترنت «مرکز» ندارد. آیا این صحت دارد؟
۳- چگونه سیستم نام حوزه، اینترنت را سازمان‌دهی می‌کند؟
۴- تفاوت بین آدرس IP و نام حوزه چیست؟
۵- تفاوت‌های عملی بین IPv4 و IPv6 چیست؟

فصل دوم

نظارت چندجانبه و چندبخشی اینترنت

هدف این بخش مرور گزارش نهایی کارگروه نظارت بر اینترنت، تنش سیاسی پیرامون جنبه‌های محتوایی نظارت بر اینترنت و ظهور مجمع نظارت بر اینترنت است.

اهمیت قانونی نظارت بر اینترنت این است که نظریه‌ها هیچ‌گاه کارکرد اینترنت را کاهش نمی‌دهند. بنابراین، کارگروه نظارت بر اینترنت چند اصل راهنما برای کار خود اتخاذ کرد، به این معنی که اینترنت باید همیشه پایدار و ایمن باشد تا معماری[1] آن و توسعه استانداردها باز و نامتمرکز باقی بمانند و اسامی و اعداد با صلاحیت مدیریت شوند.

۲-۱ تعریف

تعریف نظارت بر اینترنت با اندکی بحث آغاز می‌شود. دبیر کل اتحادیه مخابرات بین‌المللی یوشیو اوتسومی[2]، برای بررسی کارگروه نظارت بر اینترنت، به‌عنوان دبیر کل مجمع جهانی در مورد جامعه اطلاعاتی تعریف محدودی از نظارت بر اینترنت خواست. او گفت:

بسیاری از مسائلی که می‌توانند مشمول مفهوم سیاسی «نظارت بر اینترنت» شوند، در سطح وسیع در فاز اول مجمع جهانی در مورد جامعه اطلاعاتی مورد مناظره قرار گرفته‌اند و با اصول و اقداماتی که در اسناد نهایی فاز اول مطرح شده‌اند تطبیق داشته‌اند. همان‌طور که در Hammamet *گفته شد، بین دولت‌ها توافق زیادی وجود دارد که این مسائل نباید باز شوند (ادامه یابند). بنابراین به بحث درباره چنین مسائلی به‌عنوان جریان آزاد اطلاعات، مقابله با هرزنامه، امنیت شبکه، سرورهای ریشه منطقه‌ای، محافظت از حریم خصوصی یا سوءاستفاده از فناوری‌های اطلاعاتی و ارتباطاتی نیاز نیست. در عوض، ما باید روی فعالیت هسته‌ای مدیریت منابع اینترنت به‌وسیله* ICANN *به‌ویژه حوزه‌های سطح بالا که مسائل حل نشده پراهمیتی دارند؛ تمرکز کنیم.*[۳۳]

1- Architecture
2- Yoshio Utsumi

کارگروه این چشم‌انداز محدود را نپذیرفت، اما در عوض تعریف گسترده‌تری از نظارت بر اینترنت ارائه داد:

نظارت بر اینترنت، یعنی توسعه و استفاده از هنجارها، نقش‌ها، شیوه‌های تصمیم‌گیری، برنامه‌ها و اصول مشترک توسط دولت‌ها، بخش خصوصی و جامعه نظامی در نقش‌های خود که تکامل و کاربرد اینترنت را شکل می‌دهند.[۳۴]

این تعریف بخصوص در مقایسه با تعاریف پیشنهادی دیگر مختصر بود.[۳۵] تعریف از چند جهت قابل‌توجه است. اولاً، چشم‌انداز محدود نظارت بر اینترنت را با اشاره ساده به کارکردهای ICANN رد می‌کند تا اتحادیه مخابرات بین‌المللی احساس کند با آنچه که قبلاً انجام شده، مشابه است. دوماً، این تعریف مسائل سیاسی مهم عمومی مانند هرزنامه، حریم خصوصی، جرم اینترنتی، امنیت و توسعه اینترنت را پوشش می‌دهد، مسائلی که به‌راحتی با ساختار اتحادیه مخابرات بین‌المللی تطابق ندارند. سوماً، این تعریف شامل بخش خصوصی و جامعه نظامی در یک رویکرد با چندین ذی‌نفع است که اتحادیه مخابرات بین‌المللی نمی‌تواند به‌راحتی در جلسات آن شرکت کند؛ زیرا عضویت در این اتحادیه شامل شرکت‌های تلفنی است که در بسیاری از کشورها نهادهای کسب‌وکار دولتی هستند. این تعریف هم‌چنین اشاره می‌کند که نظارت بر اینترنت چیزی بیشتر از قوانین مصوب دولت است، به‌طوری‌که شامل قوانین و هنجارهای اجتماعی است که توسط جامعه اینترنتی توسعه داده شده است. این موضوع به جامعه نظامی که در توسعه اینترنت نقش دارد، رسمیت می‌دهد.

این تعریف با توضیحات بیانیه مجمع جهانی در مورد جامعه اطلاعاتی ترکیب می‌شود و اشاره می‌کند که فرآیند نظارت بر اینترنت باید دارای چندین ذی‌نفع (شامل دولت، بخش‌های عمومی و خصوصی)، چندجانبه (شامل بسیاری از کشورها) و شفاف و دموکراتیک (مطابق میل اکثریت) باشد. بنابراین اهمیت فرآیند نظارت بر اینترنت آشکار می‌شود.

۲-۲ پیشنهادها

کارگروه چندین پیشنهاد نیز داشت. اول پیشنهاد مجمع برای کلیه ذی‌نفعان جهت بررسی مسائل مربوط به اینترنت بود. مجمع یک ساختار کم هزینه بدون قدرت تصمیم‌گیری بود. هدف آن آغازی برای ذی‌نفعان جهت بحث درباره مسائل و اشتراک بهترین شیوه‌ها[1] بود. اولین مجمع نظارت بر اینترنت در آتن در سال ۲۰۰۶ تشکیل شد. جلسه دوم در ریودوژانیرو، برزیل بود. جلسه سوم در دسامبر ۲۰۰۸ در حیدرآباد، هند بود.

1- Best Practices

شکل ۱-۲ مشارکت چندجانبه و چندبخشی در نظارت بر اینترنت

منبع: DiploFoundation، http://textus.diplomacy.edu/textusbin/env/scripts/Pool/GetBin.asp?IDPool=1188.

دومین پیشنهاد کارگروه نظارت بر اینترنت بازبینی اینترنت بود. کارگروه، بین‌المللی کردن بازبینی را بر اساس اصول مجمع جهانی در مورد جامعه اطلاعاتی توصیه کرد که این بازبینی باید دارای چندین ذی‌نفع، چندجانبه، شفاف و مردمی باشد. این بازبینی نباید در عملیات روزانه اینترنت مداخله کند. کارگروه پیشنهاد داد که دولت ایالات متحده باید مرجعیت بازبینی منحصربه‌فرد خود در ICANN را رها کند.

گزارش کارگروه نظارت بر اینترنت، نه تنها ICANN را به‌عنوان شفاف‌ترین در بین آژانس‌های بین‌المللی دربرگیرنده اینترنت معرفی کرد، بلکه مسائل را نیز با ICANN توضیح داد. اول این‌که ICANN هیچ جدول زمانی هنگام ایجاد حوزه‌های عمومی سطح بالا پیشنهاد نمی‌دهد. داشتن چنین جدول زمانی برای آن‌هایی که حوزه‌های عمومی سطح بالا را پیشنهاد می‌دهند و آن‌هایی که نظری درباره حوزه‌های عمومی سطح بالای پیشنهاد شده دارند، مفید است. دوم، مشخص شد که غیر شفاف‌ترین بخش ICANN، کمیته مشاور دولت بود، مجمعی که در آن دولت‌ها ورودی‌های خود را ارائه می‌دادند. با این وجود، مسائل اصلی نظارت اول این است که ICANN یک شرکت در ایالات

متحده با یک قرارداد تک منبعی است؛ نه یک قرارداد تحت مناقصه طبق بهترین شیوه. دوم، ICANN تحت نظر اداره بازرگانی ایالات متحده با موافقت‌نامه غیررسمی است.

دولت ایالات متحده دو دلیل برای بازبینی مداوم ICANN ارائه داد: (۱) برای اطمینان از پایداری و امنیت اینترنت و (۲) برای اجتناب از سانسور اینترنت توسط دولت‌های دیگر.[۳۶] هر دو دلیل قابل‌مذاکره هستند. دلیل اول پیشنهاد می‌دهد که تخصص اداره مداوم اینترنت در بیرون از ایالات متحده آمریکا نیز وجود ندارد. دلیل دوم سانسور غیررسمی فضای نام حوزه XXX برای سایت‌های هرزه‌نگاری است که ابتدا تصویب و سپس بازبینی و رد شد. اگرچه این تصمیم توسط ICANN گرفته شد، بازبینی ظاهراً با یک گروه فشار در ایالات متحده آغاز و با یک شخص منتخب دولت ایالات متحده پشتیبانی شد.[۳۷]

اما اگر ایالات متحده آمریکا مالک اینترنت شود چه رفتاری خواهد داشت؟ در جایی که تنش بین‌المللی نسبت به نفوذ ایالات متحده وجود دارد، ممکن است دو فناوری مشابه در نظر گرفته شوند. اولی سیستم موقعیت‌یاب جهانی است (GPS)[1]، یک سرویس تحت کنترل نظامی که برای کاربرد نظامی است. اروپایی‌ها یک سیستم موازی[2] به نام Galileo توسعه داده‌اند تا اطمینان یابند اگر یک سرویس موقعیت‌یاب در دسترس باشد، ایالات متحده باید دسترسی به سیستم موقعیت‌یاب جهانی را قطع کند.[۳۸] فناوری دوم در برنامه مشترک ضد شورش[3] با نفوذ ایالات متحده است. هزینه کلی این برنامه در ۱۰ کشور، بیش از ۴۰ میلیارد دلار آمریکا و با کشورهای شریک، بیش از ۴ میلیارد دلار آمریکا برآورد می‌شود. کد منبع[4] برای برنامه کامپیوتری که برای راه‌اندازی هواپیما ضروری است، در دستان ایالات متحده آمریکاست. در ابتدا نسبت به اشتراک کد منبع حتی در پادشاهی بریتانیا که با شراکت ۵/۲ میلیارد دلاری بزرگ‌ترین سهم را در بین شرکا داشت؛ مقاومت وجود داشت. بعد از این‌که بریتانیا تهدید به ترک پروژه کرد و خرید برنامه‌ریزی شده ۱۵۰ هواپیما بی‌نتیجه ماند، دولت ایالات متحده توافقی را امضا کرد که طبق آن به بریتانیا اجازه حفظ «قدرت عملیاتی»[5] روی هواپیماها را می‌داد.[۳۹]

به‌طور خلاصه، داشتن یک سیستم موازی هزینه‌های هر دو سیستم را افزایش می‌دهد. در مورد GPS، سیستم Galileo متعهد می‌شود که دقیق‌تر از سیستم آمریکایی کار کند. اما در مورد برنامه مشترک ضد شورش، واکنش ایالات متحده یک وقفه در همکاری در برنامه‌های مشابه آتی ایجاد خواهد کرد.

1- Global Positioning System
2- Parallel System
3- Joint Strike Fighter Program
4- Source Code
5- Operational Sovereignty

سومین توصیه کارگروه نظارت بر اینترنت این بود که همکاری بین‌المللی در بین آژانس‌ها و سازمان‌های مختلف در نظارت بر اینترنت باید بهبود یابد. در بین سازمان‌های دولتی؛ اتحادیه مخابرات بین‌المللی، سازمان جهانی دارایی فکری (WIPO)[۱] و سازمان آموزشی، علمی و فرهنگی سازمان ملل (UNESCO)[۲] وجود دارند. در بین مؤسسات اینترنتی؛ ICANN، جامعه اینترنتی، نیروی کار مهندسی اینترنت[۳]، کنسرسیوم وب جهان گستر (W3C)[۴] و دفاتر ثبت اینترنت منطقه‌ای (RIRs)[۵] وجود دارند. توصیه کارگروه نظارت بر اینترنت نشان داد که علاوه بر اتحادیه مخابرات بین‌المللی تعداد زیادی آژانس دیگر نیز وجود دارد که در نظارت بر اینترنت دخالت دارند. به‌طور خلاصه، اتحادیه مخابرات بین‌المللی ادعای خاصی روی نظارت بر اینترنت نداشته است.

توصیه چهارم کارگروه نظارت بر اینترنت برای همکاری منطقه‌ای و ملی سیاست‌هاست. این توصیه یک ارتباط کاری نزدیک‌تر بین حوزه کد کشوری سطح بالا و دولت‌ها و شکل‌دهی سیاست‌های «اینترنت پسند»[۶] را پیشنهاد می‌دهد. هم‌چنین توصیه می‌کند که دولت‌ها «کمیته‌های راهبری»[۷] اینترنت را برای راهنمایی نظارت بر اینترنت راه‌اندازی کنند. این کمیته‌ها به‌ویژه برای بررسی مسائل زیر در نظر گرفته می‌شوند:

- ✓ مدیریت فایل‌های منطقه ریشه و سیستم سرور ریشه DNS
- ✓ آدرس‌دهی IP
- ✓ هزینه‌های اتصال داخلی
- ✓ پایداری، امنیت و جرم اینترنتی
- ✓ هرزنامه
- ✓ آزادی بیان[۸]
- ✓ مشارکت مفید در توسعه سیاست جهانی
- ✓ محافظت از داده و حقوق خصوصی
- ✓ حقوق مصرف‌کننده
- ✓ چندزبانگی[۹]

این مسائل در چهار دسته زیر گروه‌بندی شده‌اند:

1- World Intellectual Property Organization
2- United Nations Educational, Scientific and Cultural Organization
3- Internet Engineering Task Force
4- World Wide Web Consortium
5- Regional Internet Registries
6- Internet-Friendly
7- Steering Committees
8- Freedom of Expression
9- Multilingualism

زیرساخت فیزیکی – این دسته درباره مسائل سیاسی مانند مسائل مربوط به ICANN در رابطه با آدرس‌های IP، نام‌های حوزه و سرور منطقه ریشه بحث می‌کند. هم‌چنین مسائل مربوط به مسئولیت‌های مالی را نیز شامل می‌شود.

استفاده و سوءاستفاده از اینترنت – در این دسته مسائلی مانند هرزنامه، امنیت شبکه و جرم اینترنتی وجود دارند. بررسی چنین مسائلی باید استفاده از اینترنت را هم‌زمان با به حداقل‌رسانی سوءاستفاده، افزایش دهد.

مسائل مربوط به اینترنت ولی با تأثیر بیشتر – سیاست‌هایی که روی اینترنت اثر می‌گذارند، ممکن است روی حاشیه آن نیز تأثیر داشته باشند. مناطق کلیدی مشهود شامل سیاست رقابت، تجارت الکترونیکی و حقوق دارایی فکری هستند.

جنبه‌های توسعه اینترنت – توسعه یکی از نیروهای محرک مجمع جهانی در مورد جامعه اطلاعاتی است و بنابراین نظارت بر اینترنت می‌گوید که توسعه مسئله‌ای میان‌بر برای بحث‌هاست. سرمایه اتحاد دیجیتال[1] تسهیل استفاده از فناوری اطلاعات و ارتباطات برای توسعه (توسعه به کمک فناوری اطلاعات و ارتباطات) را آغاز کرده است. توسعه در این مفهوم باید با اهداف توسعه هزاره (MDGs)[2] هم‌راستا باشد.

این چهار دسته مسائل در بخش‌های بعدی این سرفصل بحث خواهند شد.

فعالیت

۱- سیاست‌های اینترنتی کشور خود را نام ببرید.

۲- بررسی کنید (یا به‌طور خلاصه شرح دهید) که چگونه این سیاست‌ها در کشور شما توسعه یافته‌اند؟

کشورهای در حال توسعه با دو مسئله در رابطه با اینترنت روبه‌رو هستند: (۱) چگونه مشارکت اثربخش و مفیدی در سازمان‌دهی نظارت بر اینترنت داشته باشند و (۲) چگونه ظرفیت بررسی مسائل را ایجاد کنند.

مجمع جهانی در مورد جامعه اطلاعاتی در تونس هنگامی‌که آن‌ها پیش‌بینی کردند که دولت‌های ملی تنها مرجع حوزه‌های کد کشوری سطح بالای خود هستند، با ترک برنامه‌های نظارت بر اینترنت به گزارش کارگروه نظارت بر اینترنت پاسخ داد. هرکسی که می‌خواست ادعای پیروزی داشته باشد اجازه چنین کاری را داشت.

1- Digital Solidarity Fund
2- Millennium Development Goals

جمع‌بندی:

گزارش کارگروه نظارت بر اینترنت یک خلاصه عالی از مسائل کلیدی نظارت بر اینترنت است. هم‌چنین مدلی را برای فرآیند نظارت بر اینترنت ارائه می‌دهد. این گزارش؛ دولت، بخش خصوصی و جامعه نظامی را به‌عنوان ذی‌نفعان کلیدی در نظارت بر اینترنت معرفی می‌کند. فرآیند کارگروه نظارت بر اینترنت خود یک مدل شفاف و باز بود. با این وجود، گزارش کارگروه نظارت بر اینترنت نه یک نقشه راه[1] و نه یک طرح عملی است.

خودآزمایی

۱- تعریف کارگروه نظارت بر اینترنت از نظارت بر اینترنت چیست؟ مفهوم این تعریف چیست؟
۲- توصیه‌های کلیدی کارگروه نظارت بر اینترنت چیست؟
۳- چه درس‌هایی در زمینه نظارت بر اینترنت از گزارش کارگروه نظارت بر اینترنت گرفته می‌شوند؟

1- Road Map

فصل سوم

ابعاد نظارت بر اینترنت I– استفاده از اینترنت

هدف این بخش شرح سبک‌های مختلف کنترل اینترنت است.

با اطلاع از چنین مسائلی، چگونه یک نفر نقش‌ها و سیاست‌ها را در اینترنت جایگذاری می‌کند؟ آیا کنترل اینترنت امکان‌پذیر است؟

در حقیقت، با وجود محدودیت‌ها ممکن است یک سری قوانین برای تشویق به‌کارگیری و افزایش مطلوبیت اینترنت به کار رود.

۳-۱ سبک‌های کنترل

چهار سبک زیر برای کنترل وجود دارد:

- ✓ قانون- از طریق مجوزهای دولتی و خصوصی و استفاده از زور، به انضمام خودکنترلی، بخصوص هنگام وکالت دادن به دولت؛
- ✓ هنجارهای اجتماعی- از طریق انتظارات، تشویق یا شرمندگی؛
- ✓ سازوکارهای بازار- معمولاً به قیمت و موجودی[1] می‌پردازند و
- ✓ معماری- فناوری چه مواردی را مجاز، غیرمجاز یا ممنوع می‌داند.[۴۰]

معماری

کلمه معماری به طرح فناوری اشاره دارد به‌طوری‌که رفتارهای خاص تشویق یا توبیخ می‌شوند. به‌عنوان مثال، برای توبیخ سرعت می‌توان تردد پلیس بیشتری در جاده قرار داد یا سرعت‌گیر نصب

1- Availability

کرد. در سنگاپور، جاده‌ها در نواحی مسکونی مارپیچ ساخته می‌شوند تا سرعت راننده‌ها را کاهش دهند و هم‌چنین منطقه را زیبا سازند. به‌طور مشابه، تولیدکنندگان برای جلوگیری از کپی آهنگ‌ها و ویدئوها آن‌ها را قفل و مسدود می‌کنند.

درباره اینترنت، برخی از افراد معتقدند که مقصود اصلی اینترنت افزایش آزادی بیان است. در نتیجه افرادی که خواهان کنترل هستند برای انجام این کار با چالش‌های زیادی روبه‌رو می‌شوند. در جمهوری کره، به‌جای تلاش برای کشف و دستگیری هکرها و افرادی که از بات‌نت[۱] برای حمله به اینترنت استفاده می‌کنند، آژانس امنیتی یک «هانی‌نت»[۲] برای فریب دادن بات‌نت‌ها و اتصال آن‌ها به یک شبکه قلابی توسعه داده است.

سازوکارهای بازار

این سبک کنترل، معمولاً با قیمت‌گذاری و موجودی کالاها و خدمات سروکار دارد. مقرراتی که از سازوکارهای بازار به‌عنوان ابزار کنترلی[۳] استفاده می‌کنند، شامل قوانین برابر، اصطلاحات قراردادی شفاف و پرورش رقابت در مکان بازار[۴] هستند. تجارت، در سطح مقدماتی به معنی خرید و فروش است.

حریم خصوصی تجارت در اینترنت؛ مانند دادن پست الکترونیکی فردی در عوض ارائه حقوق خواندن یا دریافت کردن محتوا؛ یک نمونه از کاربرد سازوکار بازار به‌عنوان یک نوع مقررات است. یعنی اگر فردی برای حریم خصوصی فردی دیگر بیشتر از حقوق خواندن یا دریافت محتوا ارزش قائل باشد، آدرس پست الکترونیکی او را تسلیم نخواهد کرد. در ایالات متحده آمریکا، شرکت‌های خصوصی مانند Trust-e تا محافظت از حریم خصوصی کاربران پیشرفت کرده‌اند. در مقابل، اتحادیه اروپا (EU)[۵] معتقد است که حریم خصوصی نباید با توافق خصوصی بین یک فرد و یک شرکت بلکه باید توسط قانون کنترل شود.

۱- Botnet: گروهی از کامپیوترهای متصل به اینترنت هستند که از طریق ویروس‌ها یا ضعف‌های امنیتی آلوده شده و کنترل آن‌ها در دست یک حزب مخرب قرار دارد (مترجم).

۲- Honeynet: هانی‌پات یک سیستم شبیه‌سازی شده قابل نفوذ است که از آن در شبکه‌های کامپیوتری برای جذب افراد نفوذگر و ثبت روش نفوذ آن‌ها و یا جمع‌آوری بدافزارهایی که به‌وسیله کامپیوترهای آلوده دیگر ارسال می‌شوند استفاده می‌شود. از کنار هم قرار گرفتن هانی‌پات‌ها روی زیرشبکه‌های مختلف، «هانی‌نت» به وجود می‌آید (مترجم).

3- Regulatory Tool

4- Marketplace

5- European Union

هنجارهای اجتماعی

هنگام استفاده از هنجارهای اجتماعی به‌عنوان سازوکار کنترلی، فرض می‌شود که فشار اجتماعی می‌تواند رفتار یک فرد را دیکته کند. Netiquette یا آداب معاشرت در شبکه[1] یک نمونه از استفاده از هنجارهای اجتماعی به‌عنوان یک سازوکار کنترلی است. Netiquette علاوه بر موارد دیگر، باید به مجمعی که مربوط به موضوع است پاسخ دهد و هنگام ابراز «تشکر» شما با گفتن جمله «خواهش می‌کنم» دیگر نیازی به پاسخ بیشتر ندارد.

استفاده از هنجارهای اجتماعی هنگامی‌که یک گروه اجتماعی درگیر می‌شود، به علت کارکردهای گروهی به‌عنوان عامل پایش و اجرا آسان‌تر است. افرادی که هنجارشکنی می‌کنند، ممکن است از گروه اجتماعی اخراج شوند. هنگامی‌که عضویت در گروه اجتماعی پراهمیت تلقی شود، چنین مجازاتی می‌تواند قدرتمند باشد.

قوانین، به انضمام خودکنترلی

قوانین، ظهور سیاست‌ها هستند و توسط مجلس ملی[2] و پارلمان[3] ایجاد می‌شوند. به‌طورکلی، در تصویب قوانین در یک محیط متغیر مانند فناوری، باید احتیاط شود. زیرا در این حالت، معایب پیشگامی وجود دارد. به‌عنوان مثال، قانون امضای دیجیتال یوتا[4] که در نوع خود در جهان اولین بود؛ به‌سرعت منسوخ شد، زیرا ظهور فناوری‌های جدید، رویکرد ویژه فناوری آن را قدیمی کرد. سنگاپور و ایالات متحده آمریکا که اولین قوانین مصونیت اپراتورهای شبکه[5] (در مورد سنگاپور) و واسطه‌های دیگر (در مورد ایالات متحده آمریکا) را تصویب کردند، خیلی زود پی بردند که کشورهای دیگر قوانین خود را داشته و آن‌ها را به روش‌های برتر و قابل‌بحث اصلاح نیز کرده‌اند.

شاید بهترین نصیحت این است که قوانین باید بعد از فناوری حرکت کنند و همواره رویکرد چند ذی‌نفعی را به‌روز نمایند و قبل از تصویب قوانین مشاوره کاملی داشته باشند. باید به خاطر بسپارید که اینترنت هنوز در فاز نسبتاً اولیه توسعه است.

خودکنترلی

صنعت اینترنت مایل است تا از خودکنترلی به‌عنوان روشی برای ایجاد انعطاف بیشتر در تصویب و اجرای قانون صحبت کند. در ابتدا، خودکنترلی به این معنی بود که صنعت، صنعت را تنظیم می‌کند،

1- Etiquette on the "Net"
2- National Assembly
3- Parliament
4- Utah
5- Immunize Network Operators

نه یک شخص یا یک شرکت. در عمل، خودکنترلی با دادن قدرت نهایی برای ضمانت اجرایی به دولت قدرت می‌داد. یعنی دولت به صنعت اجازه می‌دهد که در کنترل بخش مورد بحث رهبر باشد. تبلیغات ناحیه‌ای است که دولت‌ها، بخصوص کشورها مایل به استفاده از خودکنترلی هستند. دولت متخلفان بی‌اعتنا به تصمیمات صنعت را مورد پیگرد قرار می‌دهد و علیه تبلیغات گمراه‌کننده و گستاخانه آن‌ها اعمال قانون می‌کند.

با این وجود، خودکنترلی به یک بخش خصوصی برانگیخته نیاز دارد. به نظر می‌رسد کار تبلیغاتی به علت استفاده از حکم دولت[1] برای تأیید تبلیغات، حرکت این بخش تندرو را کند خواهد کرد و به احتمال زیاد خلاقیت را از بین خواهد برد. صنعت اینترنت توجه کمی به خودکنترلی دارد. حتی برخی در صنعت از این موضوع شکایت دارند که خودکنترلی به این معنی است که صنعت کار دولت را انجام می‌دهد.

پرسش‌هایی برای تفکر

۱- چهار سبک کنترل تا چه حد در کشور شما استفاده می‌شوند؟
۲- کدام سبک یا سبک‌های کنترل در کشور شما خوب جواب نمی‌دهد و چرا؟
۳- کدام سبک یا سبک‌ها بهتر جواب می‌دهند و چرا؟

۳-۲ نقشه راه پیشنهادی

از آنجایی که تعریف نظارت بر اینترنت حوزه گسترده‌ای دارد، نقشه راه زیر برای توسعه یک چارچوب سیاست[2] پیشنهاد می‌شود. نقشه راه محدوده مسائل را پوشش و فرسنگ‌شمار را نشان می‌دهد تا محکی برای تعیین کارایی قوانین و سیاست‌های در حال توسعه باشد. نقشه راه به‌قدری قدرتمند است که در برابر توسعه دنیای واقعی «آزمایش» شده است.[۴۱]

هنگامی‌که نقشه راه در سال ۱۹۹۶ ایجاد شد، بسیاری از کشورها حتی قوانین اولیه برای نظارت بر مدرک الکترونیکی[3] نداشتند. امروزه، فقط چند کشور بدون قوانین اولیه وجود دارند. با این وجود، چارچوب هنوز قابل‌اجراست زیرا راهنمایی برای پالایش قوانین و سیاست‌های در برگیرنده اینترنت است.

مسائل مورد بررسی به ترتیب اهمیت عبارتند از:

1- Government Edict
2- Policy Framework
3- Electronic Evidence

۱- تدارک خدمات و دسترسی
۲- تجارت الکترونیکی[1]
۳- کنترل محتوا
۴- امنیت
۵- حقوق دارایی فکری
۶- حریم خصوصی

ضروری است که در ابتدا به مسائل هزینه و دسترسی پرداخته شوند، زیرا با انجام این کار دسترسی به اینترنت افزایش خواهد یافت. دسترسی مسائل بسیاری در رابطه با نگاشت[2] دنیای آنلاین به دنیای آفلاین ایجاد خواهد کرد. به‌عنوان مثال، اگر کسی با استفاده از اینترنت از بانک کلاهبرداری کند، آیا قوانین مدارک به‌روز می‌شوند تا شخص بر اساس مدارک آنلاین تحت تعقیب قرار گیرد؟ یک محرک تجاری برای حل این مسائل بنیادی در تطبیق قوانین آفلاین با دنیای آنلاین وجود دارد. به علت تنش بین آنچه موجود است و می‌تواند روی اینترنت انجام شود در مقابل آنچه که موجود است و می‌تواند در دنیای آفلاین انجام شود؛ مسائل محتوایی و امنیتی ظهور می‌کنند. بسیاری از کشورها کنترل محتوای اینترنت را به‌استثنای محافظت از افراد زیر ۱۲ سال، انجام نمی‌دهند. در تصمیم کنترل محتوا و مسائل امنیتی قدری ضرورت وجود دارد، زیرا کاربران بالقوه‌ای وجود دارند که از اینترنت به این علت دوری می‌کنند که به‌عنوان مثال نمی‌خواهند در منزل دسترسی به هرزه‌نگاری وجود داشته باشد یا کامپیوترشان توسط دیگران هک شود. حقوق دارایی فکری و محافظت از حریم خصوصی با گسترش کاربرد همه‌جانبه اینترنت اهمیت بیشتری به دست می‌آورد.

تدارک خدمات و دسترسی

مسائل مورد بحث تحت این عنوان، مربوط به ایجاد دسترسی در حد توان به اینترنت هستند. این مسائل عبارتند از:

- ✓ چگونگی مدیریت استانداردهای فنی[3] در محیط شبکه
- ✓ چگونگی اتصال[4] و تعامل‌پذیری چندمحیطی[5] سیستم‌های کامپیوتری و شبکه‌ها
- ✓ چگونگی کنترل قیمت‌گذاری و کیفیت خدمات سرویس‌های اطلاعاتی
- ✓ تعیین مسئولیت‌ها و تعهدات ارائه‌دهندگان خدمات و دسترسی، مانند محافظت از دسترسی و پشتیبانی از ارائه‌دهندگان خدمات در برابر محتوای شخص ثالث[6]

1- Electronic Commerce
2- Mapping
3- Technical Standards
4- Interconnection
5- Interoperability
6- Third-Party Content

مسئله مصونیت به‌قدری اهمیت دارد که بدون آن ممکن است تجارت الکترونیکی نابود شود.

پرسش‌هایی برای تفکر

در بسیاری از کشورها، قانون افترا[1] به این معنی است که هرکس که شخص دیگری را از طریق یک عمل اشتباه[2] آزار دهد باید برای شخص آزاردیده جبران کند. در برخی از کشورها میزان مجازات ممکن است بستگی به این داشته باشد که عمل اشتباه دانسته یا نادانسته بوده است. در کشورهای دیگر، این موضوع اهمیت ندارد. در کشور شما، قوانین تا چه حد اعمال اشتباه را در (الف) یک سایت بررسی کتاب، (ب) سایت بررسی هتل و (ج) یک سایت حراجی تحمل می‌کنند؟ آیا اگر اعمال اشتباه قابل‌انتقال باشد، یک ارائه‌دهنده خدمات اینترنتی در کشور شما مسئول شناخته می‌شود؟

تجارت الکترونیکی

از دیدگاه تجاری، تجارت الکترونیکی مزایای بسیاری دارد. بنگاهی که کسب‌وکار تجارت الکترونیکی راه می‌اندازد یک مغازه شبانه‌روزی باز می‌کند که واسطه‌ها را حذف و بازارهای جدیدی ایجاد می‌کند. هم‌چنین تجارت الکترونیکی می‌تواند با خودکارسازی کسب‌وکار آن را اثربخش‌تر کند.

با این وجود، تجارت الکترونیکی برای کلیه کسب‌وکارها قابل‌استفاده نیست. تجارت الکترونیکی ممکن است برای کسب‌وکارهایی که اقلام گران مانند مبلمان می‌فروشند جواب ندهد، زیرا مشتریان معمولاً می‌خواهند این اقلام را قبل از خرید امتحان کنند. هم‌چنین، در برخی فرهنگ‌ها خرید یک فعالیت تفریحی است که تجارت الکترونیکی این جنبه را ندارد.

تلاش برای بررسی مسائل تجارت الکترونیکی ارزشمند است، زیرا با این کار گروهی از مسائل که مانع استفاده بیشتر از اینترنت هستند، حل خواهند شد. مسائل زیر باید بررسی شوند:

- ✓ سازمان‌دهی قانونی محیط الکترونیکی
- ✓ تأیید مدرک الکترونیکی
- ✓ تشخیص تراکنش‌های الکترونیکی
- ✓ تشخیص امضاهای دیجیتال و گواهی‌های دیجیتال
- ✓ حقوق، مسئولیت‌ها و تعهدات بخش‌های مختلف به‌اضافه سازوکارهای حل اختلاف
- ✓ تشویق سازوکارهای پرداخت الکترونیکی و استفاده از آن‌ها
- ✓ اختیار دادن به پلیس برای اجرای قانون در تجارت الکترونیکی

1- Law on Defamation
2- False Statement

- ✓ تعیین وضع مالیات[1] در تجارت الکترونیکی

احتمالاً لازم خواهد شد قانونی در راستای خطوطی از آنچه که به‌عنوان تجارت الکترونیکی یا قانون تراکنش‌های الکترونیکی نامیده می‌شود، وضع شود. چنین قانونی، محیطی را برای تجارت الکترونیکی آماده می‌کند.

تشخیص مدرک الکترونیکی

در بسیاری از کشورها، تشخیص مدرک الکترونیکی در اشکال مختلف آن با دسترسی گسترده عموم به اینترنت از اواسط دهه ۱۹۹۰ ضروری شده است. به‌عنوان مثال، هنگامی‌که امضاها ایجاد شدند، قوانین مدرک باید اصلاح می‌شد. در سنگاپور، قوانین توسط قانون تراکنش‌های الکترونیکی[2] در سال ۱۹۹۶ اصلاح شد. در هندوستان در سال ۲۰۰۰ قانون فناوری اطلاعات[3] را اصلاح کردند. به‌طور خلاصه، قوانین جدید دنیای آفلاین را برای کنار آمدن با دنیای آنلاین به‌روز می‌کند.

فعالیت

مقررات ایجاد یا اجرای تجارت الکترونیکی در کشور خود را شرح دهید و اگر چنین مقرراتی نباشد، فکر می‌کنید مقررات مناسب برای ایجاد یا اجرای تجارت الکترونیکی در کشورتان چیست؟

کنترل محتوا

برخی از کاربران محتوای قابل‌اعتراض[4] را به‌عنوان دلیلی برای عدم استفاده از اینترنت ذکر می‌کنند. با این وجود، آنچه قابل‌اعتراض است بین افراد مختلف متفاوت است. بنابراین حل این مسئله به ایجاد تعادل بین سلایق متناقض نیاز دارد. مزیت عمده نداشتن هرگونه فیلتر، دسترسی نامحدود به محتواست. برخی مواقع، فیلترها بیش از حد مسدود می‌کنند، بنابراین محتوای بی‌ضرر نیز مسدود می‌شود.

مسائلی که باید در کنترل محتوا به آن‌ها پرداخته شود، عبارتند از:

- ✓ چگونه موارد قابل‌اعتراض در اینترنت بخصوص به خاطر بچه‌ها، مسدود می‌شوند.
- ✓ چگونه از علایق ملی در برابر موارد نامطلوب خارجی محافظت کنیم.
- ✓ چگونه ارزش‌های فرهنگی متضاد را در محتوای اطلاعات تطبیق دهیم.

1- Taxation
2- Electronic Transactions Act
3- Information Technology Act
4- Objectionable

محتوای غیرقانونی: هماهنگی جهانی

به علت اختلافات فرهنگی، دستیابی به توافق جهانی در رابطه با تعیین موارد قابل‌اعتراض دشوار است. با این وجود، توافق بزرگ‌تری درباره آنچه که غیرقانونی است و معمولاً باعث زیان می‌شود وجود دارد. در اینجا، هرزه‌نگاری کودکان به ذهن می‌رسد.

هماهنگی جهانی[۱] با آژانس‌های اجرایی به‌عنوان یک مانع برای گسترش هرزه‌نگاری عمل کرده است. آژانس‌های اجرای قانون برای هدایت فرصت‌های طلایی با هم همکاری می‌کنند. اواخر دهه ۱۹۹۰، بیشتر تصاویر هرزه‌نگاری کودکان از دنیای آفلاین حذف شد. اما با وجود اینترنت، تصاویر زنده از سوءاستفاده از کودکان با استفاده از وب‌کم[۲] وجود دارد. برای توقف چنین سوءاستفاده‌ای، آژانس‌های پلیس افرادی را که تصاویر سوءاستفاده از کودکان را دانلود می‌کنند هدف قرار می‌دهند. تعدادی عملیات هماهنگ برجسته در سال ۱۹۹۸ (عملیات کلیسای جامع[۳]) و در سال ۱۹۹۹ (عملیات سنگ معدن[۴]) اجرا و منجر به صدها دستگیری در بسیاری از کشورها شد.

برای اطلاعات بیشتر به کارگروه نظارت بر اینترنت، گزارش پس‌زمینه[۵]، ژوئن ۲۰۰۵، ص. ۳۴، پاراگراف ۱۴۱، http://www.wgig.org/WGIG-Report.html و http://www.itu.int/wsis/documents/doc_multi.as p?lang=en&id=1661|1662|1663|1664 رجوع کنید.

امنیت

با پیشرفت کرم‌های اینترنتی[۶]، ویروس‌ها[۷] و اسب‌های تروا[۸] این مسئله اهمیت بیشتری پیدا کرده است.

ویروس «دوستت دارم»

ویروس دوستت دارم[۹]، مخرب‌ترین ویروس کامپیوتری است که سریع گسترش یافت و آژانس‌هایی مانند پنتاگون ایالات متحده، آژانس هوشمند مرکزی[۱۰] و پارلمان بریتانیا مجبور شدند سیستم پست الکترونیکی خود را برای رهایی از آن قطع کنند. علت گسترش سریع این ویروس این است که خودش را روی آدرس‌های پست الکترونیکی که در دفترچه آدرس Microsoft Outlook وجود دارند، کپی می‌کند. از آنجایی که پست‌های

1- Global Coordination
2- Webcam
3- Operation Cathedral
4- Operation Ore
5- Background Report
6- Internet Worms
7- Viruses
8- Trojan Horses
9- I love You" Virus"
10- Central Intelligence Agency

الکترونیکی از طرف آشنایان هستند، کاربران پیام را باز و ویروس را پخش می‌کنند.
با وجود هزینه زیاد پاک‌سازی[1] سیستم‌های کامپیوتری در سراسر جهان، نویسنده ویروس[2] با وجودی که شناسایی شد، قسر در رفت. وقتی‌که ویروس در می۲۰۰۰ منتشر شد، در فیلیپین؛ محل زندگی او؛ هیچ قانونی در برابر انتشار یک ویروس کامپیوتری وجود نداشت. در ژوئن ۲۰۰۰ قانون تجارت الکترونیکی فیلیپین بعد از مدت‌ها تصویب شد. این قانون شامل موادی برای متهم ساختن انتشار ویروس‌های کامپیوتری بود.
منبع: پنگ هوا آنگ[3]، «اداره کردن اینترنت آسیا»، *مجله وال استریت*[4] *آسیایی*، ۷ سپتامبر ۲۰۰۰، ص. ۸.

مسائل امنیتی اساساً عبارتند از:

- ✓ چگونه در برابر نقض امنیت در شبکه‌ها و سیستم‌های کامپیوتری محافظت کنیم.
- ✓ چگونه از جرم در محیط دیجیتال جلوگیری کنیم.

سرفصل ۶ در مجموعه سرفصل‌های *آکادمی اصول فناوری اطلاعات و ارتباطات برای مدیران ارشد دولتی* درباره «حریم خصوصی و امنیت اطلاعات» است.

حقوق دارایی فکری

دنیای دیجیتال، تهیه یک المثنی بی‌نقص را از اولین کپی ممکن می‌سازد. برخلاف دنیای آنالوگ[5] هیچ کاهش کیفیتی وجود ندارد. با این وجود، سهولت در تهیه چنین کپی بی‌نقصی به این معنی نیز هست که نقض حقوق دارایی فکری آسان است.

بنابراین سیستم جدید حقوق دارایی فکری باید به مسائل زیر بپردازد:

- ✓ چگونه سیستم جاری کپی‌رایت را برای در برگرفتن کارهای دیجیتال توسعه دهیم.
- ✓ چگونه حقوق محیط دیجیتال را کسب، محافظت و مدیریت کنیم.
- ✓ چگونه از دزدی[6] اثر دارای کپی‌رایت جلوگیری کنیم.

دزدی موسیقی

بیشترین دزدی محتوا در سطح جهان در زمینه موسیقی است. در حالی که فروش iPod و پخش‌کننده‌های دیگر موسیقی در حال ترقی هستند، چند سالی است که فروش لوح‌های فشرده[7] موسیقی کاهش پیدا کرده است. روش دزدی هنری، اشتراک همه‌جانبه و دانلود آهنگ‌ها از طریق نرم‌افزار همتا به همتا[8] است.

1- Disinfecting
2- Author of the Virus
3- Peng Hwa Ang
4- Wall Street
5- Analog World
6- Piracy
7- Compact Discs
8- Peer-to-Peer

بر خلاف تصور غلط همگان، افرادی که آهنگ‌ها را به‌صورت آنلاین به اشتراک می‌گذارند؛ می‌توانند ردیابی شوند و تحت تعقیب قانون قرار گیرند. شاید تصور غلط به این دلیل باشد که کاربران نرم‌افزار همتا به همتا مانند BitTorrent و LimeWire آهنگ‌ها را از افراد دیگر دانلود می‌کنند. بنابراین، یک نفر می‌تواند یک آهنگ را به سبک بازاریابی ویروسی[1] به افراد زیادی بدهد.

مالکان موسیقی به‌وسیله انجمن صنعت ضبط آمریکا (RIAA)[2] مقابله‌به‌مثل کرده‌اند. انجمن صنعت ضبط آمریکا دانش‌آموزانی را که می‌داند در سطح پایین مالی قرار دارند، تحت تعقیب قرار می‌دهد تا درس عبرتی برای دیگران باشد. برخی از گزارش‌ها اذعان می‌دارند که انجمن صنعت ضبط آمریکا حتی دانش‌آموزان را تشویق به ترک مدرسه کرده تا برای تسویه‌حساب کار کنند.

فعالیت

قوانین و روش‌های دیگر حفاظت از کپی‌رایت در کشور شما کدامند. تخمین بزنید که در محیط دیجیتال چقدر مؤثرند (مثلاً در زمینه توسعه فناوری دیجیتال)؟

حریم خصوصی

قوی‌ترین سیستم حریم خصوصی دستورالعمل حفاظت از داده اتحادیه اروپا[3] است که درخواست می‌کند اشخاص ثالث قبل از این‌که بتوانند داده را از اتحادیه اروپا پایش کنند، یک «سطح مناسب»[4] از محافظت از داده داشته باشند. اما اجرای آن با بی‌میلی دولت ایالات متحده برای داشتن سیستمی مشابه به تأخیر افتاده است. ایالات متحده شرط «پناهگاه ایمن»[5] را به‌عنوان جایگزین خلاقانه پیشنهاد داد که در آن افرادی که مطابق دستورالعمل هستند در پناهگاه ایمن قرار دارند و فرض می‌شود که موافق دستورالعمل نیز هستند.

سازمان توسعه و همکاری اقتصادی (OECD)[6] نیز رهنمودهایی برای حریم خصوصی ارائه داده است که تلاش می‌کند وضعیت آسان‌تری برای حریم خصوصی، در مقایسه با وضعیت اتحادیه اروپا در حریم خصوصی ایجاد کند.[۴۲]

مسئله اصلی در مقررات حریم خصوصی این است که چگونه استفاده از اطلاعات شخصی توسط مؤسسات خصوصی و عمومی کنترل شود.

1- Viral-Marketing Fashion
2- Recording Industry Association of America
3- EU's Data Protection Directive
4- Adequate Level
5- "Safe Harbour" Provision
6- Organization for Economic Co-Operation and Development

مطابقت با استانداردهای اتحادیه اروپا

وضعیت اتحادیه اروپا در زمینه حریم خصوصی به‌خوبی مورد مطالعه قرار گرفته است. بخشی از رویکرد جدید آن این شرط است که داده اتحادیه اروپا نمی‌تواند به کشوری دیگر برای پایش ارسال شود، مگر این‌که آن کشور در محافظت از داده با اتحادیه اروپا هم‌سطح باشد. در عمل، استثناهایی وجود دارد مانند پروازهای هواپیمایی. اما سیاست اتحادیه اروپا بسیاری از کشورها را وادار کرده است تا قوانین محافظت از داده را برای تطابق با استانداردهای اتحادیه اروپا به‌روزرسانی کنند.

شکی وجود ندارد که استاندارد اتحادیه اروپا مقداری هزینه به کسب‌وکار تحمیل می‌کند. بنابراین به‌طور قابل‌درک انجمن‌های کسب‌وکار سعی می‌کنند تا حداقل استاندارد را هر جا که امکان دارد، رعایت کنند.

ایالات متحده شروط پناهگاه ایمن را که توسط دولت ایالات متحده تا حدودی مورد مذاکره قرار گرفته بود، دارد، اگرچه به‌ظاهر این کار توسط بخش خصوصی انجام شده بود. شرط پناهگاه ایمن ایالات متحده به این معنی است که شرکت‌هایی که استانداردهای محافظت از داده آن‌ها مطابق با استانداردهای پناهگاه ایمن خودکنترلی است قادر خواهند بود داده را از اتحادیه اروپا دریافت و پایش کنند.

در استرالیا، دولت تلاش کرد قوانین حریم خصوصی را به‌روز کند تا به سطح «مناسب»[1] با اتحادیه اروپا برسد. با این وجود، ظاهراً به علت اعمال نفوذ[2] کسب‌وکار، شروط تضعیف شدند و کمبود امنیت به وجود می‌آمد.

بنابراین برای پایدار بودن باید بین علایق کسب‌وکار و استاندارد اتحادیه اروپا در محافظت از داده تعادل وجود داشته باشد.

صفحات وب کمیسیون اروپایی در محافظت از داده در http://ec.europa.eu/justice_home/fsj/privacy/index_en.htm لینک‌هایی برای منابع و اطلاعات بیشتر در زمینه حریم خصوصی دارند.

جمع‌بندی:

رویکردهای مسائل مربوط به اینترنت که در بالا خلاصه شده‌اند، بر اساس هنجارهای بین‌المللی هستند؛ زیرا حوزه اینترنت بین‌المللی است و هیچ کشوری نمی‌تواند از بقیه جامعه بین‌المللی جدا باشد. به‌علاوه، لازم است که با ذی‌نفعانی همچون جامعه نظامی و صنعت به‌طور گسترده، چه در آموزش دادن جامعه و چه در آموزش دیدن درباره مسائل، مشاوره شود.

1- Adequate
2- Lobbying

فعالیت

تعیین کنید آیا رتبه‌بندی شش دسته از مسائل بالا برای کشور شما مناسب هستند یا خیر. اگر احساس می‌کنید رتبه‌بندی داده شده مناسب کشور شما نیست، پیشنهاد دهید چگونه این دسته از مسائل باید برحسب درجه اهمیت در کشور شما رتبه‌بندی شوند و پیشنهاد خود را توجیه کنید.

خودآزمایی

۱- چهار سبک کنترل اینترنت کدامند؟ محدودیت‌های آن‌ها در ارتباط با کنترل اینترنت چیست؟

۲- نقشه راه پیشنهاد شده برای کنترل اینترنت فقط یک راهنمای پیشنهادی است. مراحل پیشنهادی این نقشه راه کدامند؟

فصل چهارم

ابعاد نظارت بر اینترنت II– استفاده از اینترنت

هدف این بخش افزایش آگاهی در زمینه سوءاستفاده‌های معمول از اینترنت و اقداماتی است که می‌توان به آن‌ها پرداخت.

٤-١ ویژگی خاص اینترنت چیست

برخی تعبیر کرده‌اند که اینترنت صرفاً بازتاب دنیای آفلاین است و بنابراین به قوانین خاصی برای آن نیاز نیست. با این وجود، چند ویژگی خاص برای اینترنت وجود دارد.

اولاً، اینترنت ناشناس ماندن را آسان‌تر می‌کند. امکان دارد برای اطمینان از اجرای قانون کاربران ردیابی شوند. اما انجام این کار نیاز به تلاش و منابع ویژه‌ای دارد. قدرت گمنامی در این است که باعث ارتباطات باز و بی‌پرده در مواردی مانند شرایط پزشکی می‌شود. با این وجود، گمنامی ممکن است پوششی برای مجرمان نیز باشد.

دوماً، فرهنگ هرج و مرج و بی‌قانونی در اینترنت وجود دارد که جان پری بارلو[1] در «بیانیه استقلال فضای سایبری»[2] به بهترین شکل آن را شرح می‌دهد:

دولت‌های جهان صنعتی، شما غول پیکرانی از گوشت و فولاد هستید، من اهل فضای سایبری هستم، خانه جدید ذهن. از طرف آینده، از شما درباره گذشته سؤال می‌کنم که ما را تنها گذاشتید. شما در بین ما جایی ندارید. شما قدرتی در جایی که ما جمع می‌شویم ندارید.[۴۳]

البته این بیانیه «نقشه خیالی»[3] موهوم و خالی از امیدی بود که عدم درک قوانین را منعکس می‌کرد: قوانین بر افراد یک مکان نظارت می‌کنند، نه خود مکان. تا زمانی که افراد وجود دارند، همواره

1- John Perry Barlow
2- Declaration of the Independence of Cyberspace
3- Pipedream

نیاز به قوانین برای توضیح حقوق و اقدام به‌عنوان تسهیل‌کننده اجتماعی برای به حداقل‌رسانی اختلافات افراد وجود دارد.

سوماً، در شروع یادگیری، اینترنت ابزاری قوی برای شبکه‌سازی است. این ظرفیت که در سایت‌های شبکه اجتماعی مانند Myspace و Facebook به بهترین شکل شرح داده می‌شود؛ در حال حاضر به‌عنوان وب ۲/۰ شناخته می‌شود. با وب ۲/۰ گروه‌های ویژه[1] کوچک ممکن است جمع شوند و جوامع بسیار بزرگی در جهان به وجود آورند. یک مثال barefooters.org است که اعضای آن به‌جز در موقعیت‌های رسمی پابرهنه راه می‌روند. در سال ۱۹۹۹، فقط ۴۰۰ نفر از آن‌ها در سطح جهان وجود داشتند. در سال ۲۰۰۷، به ۲۰۰۰ نفر در چندین کشور رسیدند. در سطح جهانی، گروه بزرگی از کاربران را در اختیار داشتند تا لوگوی خود را داشته باشند.

اینترنت؛ همان‌طور که در زیر بحث می‌شود؛ به روشی مشابه به افرادی که تلاش می‌کنند تا خراب‌کاری و ایجاد مزاحمت کنند، کمک می‌کند.

۲-٤ سوءاستفاده از اینترنت

هرزه‌نگاری کودکان

در ابتدا هرزه‌نگاری کودکان تبدیل نسخه چاپی[2] محتوا به نسخه‌های غیرچاپی[3] بود. اما با بهره‌برداری از فناوری، امکان تقاضا برای هرزه‌نگاری به وجود آمد که طبق آن هرزه‌نگاری کودکان بنا به تقاضا تولید می‌شد.[۴۴]

برای متلاشی کردن گروه‌های مجرمی که هرزه‌نگاری کودکان را ترویج می‌دهند، مشارکت بین‌المللی لازم است. دو نمونه از چنین مشارکت بین‌المللی هجوم هم‌زمان چند کشور توسط پلیس بین‌الملل در طول عملیات کلیسا در سال ۱۹۹۹ و عملیات سنگ معدن در سال ۲۰۰۲ بود که شبکه‌های هرزه‌نگاری کودکان را منحل کردند.[۴۵] در این مورد مشارکت بین‌المللی امکان‌پذیر است، زیرا هرزه‌نگاری کودکان یکی از معدود مواردی است که توافق جهانی در مورد مجرمانه بودن آن وجود دارد.

کلاهبرداری از مصرف‌کننده

اینترنت نشان داده است که برخی مواقع قوانین آفلاین باید برای کنار آمدن با اقتصاد تغییر کنند. یک نمونه، قوانین حراجی[4] هستند. در بسیاری از کشورهای مشترک‌المنافع[5] حراجی نیاز به

1- Niche Groups
2- Hardcopy
3- Softcopies
4- Auction
5- Commonwealth

حضور فیزیکی فرد با یک مجوز حراجی دارد. در نگاه اول، چنین قانونی بسیار قدیمی به نظر می‌رسد. به این معنی که مثلاً حراج‌کنندگان eBay باید برحسب داشتن یا نداشتن مجوز بررسی شوند. با این وجود، منطق این قانون با آزاد کردن حراجی‌های الکترونیکی خیلی سریع روشن شد: کلاهبرداری در حراجی که یکی از بزرگ‌ترین کلاهبرداری‌های آنلاین است.[۴۶]

کلاهبرداری از مصرف‌کننده یکی دیگر از حوزه‌هایی است که توافق بین‌المللی برای توقف آن وجود دارد. از بین بردن چنین کلاهبرداری‌هایی می‌تواند سودمندی[۱] اینترنت را افزایش دهد. از سال ۱۹۹۶، یک پالایش سالانه در اینترنت برای کلاهبرداری از مصرف‌کننده وجود داشته است. تعداد کشورهایی که در این پالایش وجود دارند، در حال افزایش است.

پالایش سالانه مصرف‌کننده

حدود ۴۰ کشور با یکدیگر متحد شده‌اند تا کلاهبرداری آنلاین مصرف‌کننده[۲] را تحت شبکه بین‌المللی تقویت و پشتیبانی از مصرف‌کننده (ICPEN)[۳] بررسی کنند. این شبکه یک روز پالایش اینترنتی بین‌المللی[۴] را در سال برای پاک‌سازی آن دسته از وب‌سایت‌های اینترنتی در نظر گرفته که ادعای زیادی دارند. پالایش‌ها به‌ویژه کلاهبرداری و اسکم را هدف قرار می‌دهند.

باید توجه شود که چنین پالایش‌هایی دقیقاً مانند قوانین آفلاین پشتیبانی از مصرف‌کننده، کار می‌کنند. بنابراین کشورهای توسعه یافته در چنین پالایش‌هایی فعال‌ترند.

جزییات بیشتر درباره شبکه بین‌المللی تقویت و پشتیبانی از مصرف‌کننده و فعالیت‌های آن در http://www.icpen.org وجود دارد.

پرسش‌هایی برای تفکر

قوانین ضد هرزه‌نگاری کودکان و کلاهبرداری از مصرف‌کننده در کشور شما چگونه اثربخش هستند؟

هرزنامه، اسکم، کد مخرب، فیشینگ

مسئله‌ای که به‌عنوان تقویت تدریجی اهداف سیاسی و تجاری دیده می‌شود، هرزنامه یا تجمع پست الکترونیکی تجاری ناخواسته است. دلیل آن این است که هرزنامه پهنای باند[۵] را هدر می‌دهد.

1- Utility
2- Consumer Fraud Online
3- International Consumer Protection and Enforcement Network
4- International Internet Sweep Day
5- Bandwidth

مهم‌تر از این، هرزنامه می‌تواند یک تهدید امنیتی قابل‌توجه باشد زیرا ممکن است کد مخرب به همراه داشته و باعث فیشینگ[۱] شود که فیشینگ «فرآیند تلاش برای کلاهبرداری مجرمانه جهت دستیابی به اطلاعات حساس مانند نام‌های کاربری، رمزهای عبور و جزییات کارت اعتباری با تغییر قیافه[۲] به‌عنوان یک موجودیت قابل‌اعتماد[۳] در یک جامعه الکترونیکی» است.[۴۷]

اینترنت به علت ریشه‌هایی که در دانشگاه دارد، با یک فرهنگ باز و قابل‌اعتماد آغاز شده است. در اولین روزها هنگامی‌که کاربران (که اغلب در دانشگاه‌های ایالات متحده بودند) به لیست‌های پست الکترونیکی خود پیام ارسال می‌کردند، بسیاری از افراد شماره تلفن خود را بعد از امضا قرار می‌دادند؛ تا نشانه‌ای از صحت آنچه که پست کرده‌اند باشد. امروزه، با دسترسی گسترده به اینترنت، گذاشتن شماره تلفن در پیام پست الکترونیکی کلیه روش‌های حمله[۴] را جذب می‌کند.

اولین هرزنامه احتمالاً توسط نماینده بازاریابی شرکت تجهیزات دیجیتال (DEC)[۵] فرستاده شد. این شرکت کامپیوترهای کوچک[۶] برای اینترنت می‌ساخت. این هرزنامه، یک پیام تبلیغاتی تجاری برای نمایش محصول بود. کاربران شکایت کردند و برخلاف امروزه که فرستندگان هرزنامه به‌راحتی ردیابی نمی‌شوند؛ برخورد قانونی با فرستندگان صورت گرفت.[۴۸]

در حالی که بیشتر هرزنامه‌های شناسایی شده امروزی از نوع هرزنامه پست الکترونیکی هستند، این اصطلاح در سوءاستفاده‌های مشابه در ابزارهای دیگر اینترنتی مانند پیام‌رسانی آنی[۷]، گروه خبری یوزنت[۸]، موتور جست‌وجوی وب[۹]، وبلاگ‌ها[۱۰]، ویکی‌ها[۱۱]، پیام‌رسانی تلفن همراه[۱۲] و بازی‌ها نیز استفاده می‌شود. هرزنامه پست الکترونیکی در سطح بین‌الملل به‌عنوان «تجمع پست الکترونیکی ناخواسته»[۱۳] تعریف می‌شود: پست الکترونیکی بخشی از مجموعه بزرگ‌تری از پست‌های الکترونیکی ماهیتاً یکسان است که گیرنده مایل به دریافت آن نیست.[۴۹] پس قانون‌گذاری[۱۴] برای هرزنامه باید رضایت[۱۵] را مخاطب قرار دهد نه محتوا را.

1- Phishing
2- Masquerading
3- Trustworthy Entity
4- Manner of Attacks
5- Digital Equipment Corporation
6- Mini-Computers
7- Instant Messaging
۸- Usenet Newsgroup: بخشی از اینترنت که هر کاربر می‌تواند پیامی بیفزاید یا به پیام‌های دیگر مطالبی اضافه کند (مترجم).
9- Web Search Engine
10- Blogs
11- Wikis
12- Mobile Phone Messaging
13- Unsolicited Bulk e-Mail
14- Legislation
15- Consent

هرزنامه کی به پایان خواهد رسید

مسئله هرزنامه این است که برخلاف تبلیغات سنتی، اکثر هزینه‌های آن به دوش گیرنده است، نه فرستنده. مطالعات مختلف پیشنهاد می‌دهند که بیشتر ترافیک پست الکترونیکی مربوط به هرزنامه است.

اولین نسل هرزنامه شامل آزار و اذیت‌هایی بود که غالباً کاربران و سیستم‌های مدیر می‌توانستند آن‌ها را فیلتر کنند. نسل جدیدتر هرزنامه هشداردهنده است. امروزه هرزنامه‌ها به‌طور فزاینده‌ای کد مخرب نرم‌افزاری به همراه دارند که بدون اطلاع کاربر اجرا می‌شوند. سپس کامپیوتر ممکن است به یک «بوت»[۱] تبدیل شود که توسط فرستنده هرزنامه کنترل می‌شود. در برخی نمونه‌ها، هرزنامه ممکن است کدی را برای بازیابی رمزهای عبور و دیگر داده‌های حساس به همراه داشته باشد.

پیچیدگی[۲] و مقیاس این عملیات سطحی از سازمان را که اغلب مربوط به گروه بزهکاران است، پیشنهاد می‌دهد.

اولین قانون در جهت شمول هرزنامه قانون «هرزنامه می‌تواند»[۳] آمریکا[۴] در سال ۲۰۰۳ بود. نام کامل آن «قانون کنترل حمله هرزه‌نگاری و بازاریابی ناخواسته»[۵] است. این مصوبه اختیارات اقدام قانونی را به شهروندان خصوصی واگذار می‌کند و برای پیگیری اپراتورهای شناخته شده هرزنامه در ایالات متحده آمریکا مورد استفاده قرار گرفته است. ارزیابی این مصوبه در سال ۲۰۰۵ انجام شد و تغییر قابل‌توجهی در آن صورت نگرفت. با این وجود، سطح هرزنامه در ایالات متحده به‌قدری است که رتبه اول یا دوم هرزنامه را در سطح جهان دارد. چین یا جمهوری کره نیز رتبه بالایی دارند.

به نظر می‌رسد که هرزنامه در جاهایی که نفوذ اینترنت بیشتر است؛ مانند جمهوری کره و جاهایی که قوانین و اجرای ضعیفی دارند؛ مانند چین، پیشرفت می‌کند.

تا زمانی که تولیدکنندگان هرزنامه با شکست روش‌های قبلی خود، روش‌های پیشرفته‌تری ایجاد می‌کنند، بازی موش و گربه ادامه دارد. انواع مختلفی از همبستگی‌ها، گروه‌های کاری و گروه‌های ذی‌نفعان متقاضی بعد از سال ۲۰۰۳ برای پرداختن به این مسئله به وجود آمده‌اند. در اواخر سال ۲۰۱۱ فعال‌ترین گروه، کار گروه ضد سوءاستفاده از پیام‌رسانی (MAAWG)[۶] بود که یک مسئول اجرایی تمام وقت با دفتری در سان‌فرانسیسکو در ایالات متحده آمریکا دارد. برخلاف گروه‌بندی‌های پیشین که صرفاً متمایل به تمرکز روی هرزنامه پست الکترونیکی بودند؛ کار گروه ضد سوءاستفاده از پیام‌رسانی یک چشم‌انداز کل‌نگر ایجاد کرد تا هرزنامه را در ابزارهای جدید مانند سرویس پیام کوتاه (SMS)[۷] و سایت‌های شبکه اجتماعی نیز بررسی کند.[۵۰]

۱- Bot: عنکبوت یا ربات جست‌وجوگر که مطالب و عکس‌های کامپیوتر شما را عنکبوت‌وار جست‌وجو می‌کند (مترجم).

2- Sophistication
3- CAN-SPAM
4- American CAN-SPAM Act
5- Controlling the Assault of Non-Solicited Pornography and Marketing Act
6- Messaging Anti-Abuse Working Group
7- Short Message Service

مزاحمت سایبری، کمین سایبری، سرقت هویت، اعتیاد به اینترنت

مضرات این بخش ناشی از استفاده آنلاین است. هنگامی‌که یک فرد زمان زیادی را آنلاین است، احتمال وقوع این خطرات بیشتر است. مزاحمت سایبری[1] آزار یک خردسال توسط خردسال دیگر با استفاده از اینترنت و وسایل ارتباطی الکترونیکی[2] دیگر اغلب شامل ارسال پیام‌های تحقیرآمیز و توهین‌آمیز است. اگر مزاحمت توسط شخصی بزرگسال صورت گیرد، آزار سایبری[3] نامیده می‌شود.

کمین سایبری[4] استفاده از اینترنت و وسایل ارتباطی الکترونیکی دیگر برای کمین کردن قربانی است که اغلب به دنبال کمین کردن آفلاین اتفاق می‌افتد؛ اما می‌تواند مقدمه کمین کردن آفلاین نیز باشد.

سرقت هویت[5] شامل استفاده از جزییات شخصی برای برخی منافع یا اجتناب از برخی الزامات است. یک نمونه متداول استفاده از جزییات شخصی قربانی برای دستیابی به کارت اعتباری است.

زیان ناشی از این شرارت ممکن است جدی باشد؛ مانند زمانی که یک کمین‌کننده سایبری، قربانی مؤنثی را که در کمینش بوده است می‌کشد. راه‌حل تصویب قوانینی برای مبارزه با آن‌هاست.

اعتیاد به اینترنت یعنی استفاده بیشی از حد از اینترنت که معمولاً به زیان مدرسه یا محل کار است. جمهوری کره سرویس مشاوره جدید برای بررسی این مسئله دارد.

بررسی اعتیاد به اینترنت

اعتیاد به اینترنت به‌عنوان یک اختلال وسواسی[6] مانند اعتیاد به قمار در نظر گرفته می‌شود. افراد معتاد ممکن است ۱۷ تا ۱۸ ساعت در روز را در اینترنت بگذرانند. کشورهایی که بیشترین معتادان اینترنتی را دارند شامل چین، ژاپن، جمهوری کره و تایوان هستند. از آنجایی که بسیاری از معتادان اینترنتی در آسیا هستند، این سؤال به وجود می‌آید که عوامل فرهنگی چقدر روی این رفتار وسواسی تأثیر می‌گذارند. تحقیقات بیشتر تعیین می‌کنند که آیا یک اختلال مظهر اختلالات وسواسی دیگر است یا خیر.

ویکی‌پدیا در «اختلال اعتیاد اینترنتی» (http://en.wikipedia.org/wiki/Internet_addiction_disorder) گزارش معقول متعادلی از نظرات موافق و مخالف پدیده اعتیاد ارائه می‌دهد.

1- Cyberbullying
2- Electronic Means of Communication
3- Cyberharassment
4- Cyberstalking
5- Identity Theft
6- Compulsive Disorder

فعالیت

سطح آگاهی نسبت به هرزنامه، اسکم، فیشینگ، مزاحمت سایبری، کمین سایبری، سرقت هویت و اعتیاد اینترنتی در سازمان، دولت و جامعه خود را به‌طور رسمی ارزیابی کنید. برای ارزیابی خود مدرک یا دلیل ارائه دهید.

تمایل سیاسی

نزاع با این کاربردهای منفی نیاز به تمایل سیاسی[1] دارد. اولاً، اعمال مورد بحث باید در کشور قانونی باشند. در برخی از کشورها، قوانین پشتیبانی از مصرف‌کننده آن‌قدر ضعیف‌اند که اجرای آن‌ها غیرممکن یا بی‌نتیجه است. دوماً، باید تمایل سیاسی در سطح بین‌المللی برای مشارکت وجود داشته باشد. به‌عنوان مثال، اسکم ۴۱۹ نیجریه[2] ادامه پیدا می‌کند زیرا دولت نیجریه عملاً هیچ اقدامی علیه آن انجام نمی‌دهد. نتیجه سطح پایین اعتماد در تجارت الکترونیکی نیجریه است.[۵۱]

پیش‌پرداخت حق‌الزحمه یا کلاهبرداری ۴۱۹ نیجریه

متأسفانه نیجریه که در پایین شاخص‌های جهانی فساد قرار دارد، در یک کلاهبرداری آنلاین عمومی به نام بعد از یک شرط[3] در قوانین جزای خود در برابر دستیابی به دارایی با ادعای کذب شرکت کرد. اسکم ۴۱۹ نیجریه یک کلاهبرداری پیش‌پرداخت حق‌الزحمه[4] است که قربانی باید در ازای دریافت مبلغ قابل‌توجهی، مقداری وجه ارسال کند

یک پست الکترونیکی معمولی برای قربانی از طرف فردی با مقداری وجه که نمی‌تواند بدون کمک، به آن دسترسی داشته باشد می‌آید. این مبلغ معمولاً از طرف وارث یک رییس معزول، یک حساب بانکی مسدود یا حتی مقداری رشوه[5] است. از کسی که در دام می‌افتد درخواست می‌شود مبالغ زیاد و زیادتری برای مسائل پیش‌بینی نشده ارسال کند.

به علت مجموع مبالغ در نظر گرفته شده، این عملیات اغلب به‌صورت حرفه‌ای با تبانی مقامات رسمی دولت سازمان‌دهی می‌شوند. برخی از افرادی که برای بررسی به نیجریه رفته‌اند مفقود شده یا به قتل رسیده‌اند.

ویکی‌پدیا در «کلاهبرداری پیش‌پرداخت حق‌الزحمه» (http://en.wikipedia.org/wiki/Advance-fee_fraud) خلاصه تاریخچه اسکم و جزییات متغیرهای آن را آورده است.

1- Political Will
2- Nigerian 419 Scam
3- After a Provision
4- Advance-Fee
5- Bribe

۳-٤ مجازات

هر بحثی در نظارت باید اجرای قوانین را در نظر بگیرد. بدون اجرا، قوانین در بهترین حالت تبدیل به آرمان و در بدترین حالت آلتی برای تمسخر عیب‌جویان می‌شوند. این بخش بررسی می‌کند که چگونه مجازات[1] برای اجرای قوانین اینترنتی مورد توافق به کار می‌روند.

هنجارهای جامعه سایبری: مجازات عمومی و Netiquette

جوامع سایبری ممکن است سنت‌ها، هنجارها و قوانین Netiquette خاص خود را برای اجرا داشته باشند. در چنین مواردی، بیشترین سخت‌گیری از طرف مجازات عمومی[2] شامل تبعید و اخراج اجتماعی است.

با این وجود، این نوع مجازات اجتماعی نادر هستند، زیرا اغلب کسب توافق درباره اشتباه بودن یک عمل و توافق درباره میزان اشتباه و مقدار مجازات دشوار است. هم‌چنین، مجازات تبعید اجتماعی ممکن است تنبیه کافی برای برخی افراد نباشد. به‌طور خلاصه، مجازات اجتماعی جواب می‌دهند اما به روش‌های محدود.

کمک به خود

در برخی موارد، امکان دارد گروه آسیب‌دیده به روش کمک به خود[3] متوسل شود. به‌عنوان مثال مالکان کپی‌رایت سابقه استفاده از کمک به خود را دارند، آن‌ها افرادی را که به حقوق کپی‌رایت آن‌ها تجاوز می‌کنند تحت تعقیب قرار می‌دهند و در حقیقت سیستم اجرایی این روش را ایجاد می‌کنند. یعنی بیشتر کارها در زمینه بررسی و اجرای اقدامات قانونی توسط مالکان کپی‌رایت انجام می‌شود و حتی اگر قوانین کپی‌رایت تحت مواد مجرمانه باشد، پلیس اقدامی نمی‌کند.

در سال ۲۰۰۰، کمیته المپیک سیدنی یک شرکت خصوصی به نام خدمات کنترل کپی‌رایت را اجاره کرد؛ تا اینترنت را برای کشف سایت‌های غیرمجازی که اخبار المپیک را پخش می‌کنند، جست‌وجو کند. دلیل این کار این بود که حقوق پخش نتایج به بالاترین پیشنهادکننده[4] به مبلغ ۲۰۰ میلیون دلار آمریکا فروخته شده بود و هر رخنه غیرمجاز موفقیت پیشنهاددهنده را کاهش می‌داد. حدود ۶۰ نفر که اینترنت را جست‌وجو می‌کردند، در متوقف ساختن پخش‌کننده‌های غیرمجاز بزرگ موفق بودند. یک ایستگاه تلویزیونی روسی (شبکه ۶ مسکو)[5] هنگامی‌که منبع ویدئوی اینترنتی را راه

1- Sanctions
2- Community-Administered Sanctions
3- Self-Help
4- Bidder
5- Moscow TV6

انداخت، درباره آزادی بیان صحبت کرد. اما شبکه ۶ مسکو مجبور بود پخش غیرمجاز خود را متوقف کند زیرا به آن‌ها گفته شد که اگر ادامه دهند ویدئوی که به ایستگاه تلویزیون متصل بود؛ قطع خواهد شد.[۵۲] از آن به بعد، در المپیک‌های تابستانی و زمستانی بازرسی انجام می‌شود.

قانون بین‌المللی

صحبت‌هایی درباره ایجاد قانون بین‌المللی برای بازرسی و پیگرد قانونی جرم‌های سایبری وجود داشته است. چنین قانونی ماهیتاً یک کد یکسان[1] برای تعیین، تعقیب و اجرای قوانین علیه جرم‌های سایبری ایجاد می‌کرد. مشارکت بین‌المللی در این زمینه وجود دارد، اما فقط شامل چند کشور است.

شورای کنوانسیون اروپا در زمینه جرم سایبری[2] یک تلاش منطقه‌ای برای چنین کدی است. از آنجایی که اروپا به‌قدر کافی تنوع دارد، کنوانسیون می‌تواند برنامه‌های کاربردی گسترده‌تری داشته باشد. کنوانسیون بین نیاز به اجرا و آزادی بیان نیز تعادل برقرار می‌کند.

شورای کنوانسیون اروپا در زمینه جرم سایبری

آژانس‌های اجرای قانون برای اثربخشی در فضای سایبری باید سهولت را نیز در نظر بگیرند، زیرا اینترنت مرزها و حوزه‌ها را قطع می‌کند. یعنی اگر آژانس‌های اجرای قانون روی قوانین جهانی توافق نداشته باشند، دستیابی به گروه مجرمان مسئله خواهد شد.

با این وجود، جامعه اینترنت در اجرای قانون تنوع دارد. در اینترنت فرهنگ «تقریباً هر چیزی عبور می‌کند»[3] وجود دارد که در آن آزادی بیان ارزشمند است. نظر به این‌که اینترنت هنوز در مرحله ابتدایی است، این نگرانی نیز وجود دارد که قوانین مصوب ممکن است مانع توسعه آن شوند.

شورای کنوانسیون اروپا در زمینه جرم سایبری تلاش می‌کند این نگرانی‌ها را بررسی کند. شورای اروپا (CoE)[4] شامل تقریباً کلیه کشورهای اروپایی است. این شورا نسبت به اتحادیه اروپا که سازمانی متفاوت است اعضای بیشتری دارد. شورای اروپا قراردادهایی منعقد می‌کند که ممکن است اعضا تصویب نکنند، در حالی که اتحادیه اروپا بیانیه‌هایی منتشر می‌کند که اعضای آن باید آن را به تأیید قانون محلی برسانند.

به علت تعداد زیاد کشورهای درگیر (حدود ۵۰ کشور)، انعقاد قرارداد جرم سایبری مسائل زیادی به وجود می‌آورد. اما چون شورای اروپا یک سازمان منطقه‌ای است، فرهنگ نزدیک‌تر و هم‌جواری فیزیکی به این معنی است که تنش‌های دیپلماتیک در بحث روی این مسائل به حداقل می‌رسند. هم‌چنین، طبیعت قراردادها به این صورت

1- Uniform Code
2- The Council of Europe Convention on Cybercrime
3- Almost Anything Goes
4- Council of Europe

است که کشورها ممکن است روی متن با هم توافق داشته باشند اما نمی‌توانند انتخاب کنند[1] یا ممکن است به‌صورت گزینشی انتخاب کنند. این توانایی انتخاب قدرت تصمیم‌گیری در رابطه با قانون را در دستان مجلس ملی[2] قرار می‌دهد. در مقابل، قوانین مصوب مجلس اتحادیه اروپا باید به‌عنوان قانون قوه مقننه ملی اجرا شوند.
بنابراین قوانین شورای اروپا موازنه‌ای بین نگرانی‌های مختلف به وجود می‌آورند. کنوانسیون جرم سایبری چندین دوره بازبینی بین‌المللی با ورودی‌های سازمان‌هایی مانند اتحادیه آزادی مدنی آمریکا[3] در رابطه با چالش‌های بالقوه آزادی بیان انجام داد. کنوانسیون رهنمودهایی برای کشورها به‌منظور اجرای قوانین جرم سایبری ارائه می‌دهد. این کار در ژولای ۲۰۰۴ آغاز شد. ماده‌ای برای مشارکت بین‌المللی وجود دارد که به این معنی است که کشورهایی که جزء شورای اروپا نیستند، می‌توانند به کنوانسیون ملحق شوند. در حقیقت، اجرای آن در ژانویه ۲۰۰۷ در ایالات متحده آمریکا آغاز شد.
برای اطلاعات بیشتر به "شورای اروپا، جرم سایبری: یک تهدید علیه دموکراسی، حقوق بشر و قانون"، http://www.coe.int/t/dc/files/themes/cybercrime/default_en.asp مراجعه کنید.

پرسش‌هایی برای تفکر

کشور شما تا چه حد در مشارکت بین‌المللی برای رسیدگی به سوءاستفاده از اینترنت همکاری می‌کند؟

جمع‌بندی:

هیچ شکی وجود ندارد که بسیاری از قابلیت‌های اینترنت که آن را تبدیل به ابزاری نیرومند کرده‌اند، دلیل استفاده از آن برای اهداف سوء نیز هستند. تردیدی وجود ندارد که باید برخی از این کاربردهای نادرست از اینترنت کنترل شوند.

به علت دشوار بودن کسب توافق در تعریف جرم در سطح جهانی، موفقیت اندکی در بررسی برخی از آزار و اذیت‌های اینترنتی وجود دارد. اغلب موفقیت‌های قابل‌توجه در کلاهبرداری از مصرف‌کننده و هرزه‌نگاری کودکان است.

توافق بین‌المللی برای اولاً تصویب قوانین و سپس برای اجرای آن‌ها ضروری است. شورای کنوانسیون اروپا در زمینه جرم سایبری ممکن است زیرساختی برای مشارکت و توافق آتی باشد.

1- Opt-in
2- National Parliament
3- American Civil Liberties Union

خودآزمایی

۱- آژانس‌های بین‌المللی در بررسی سوءاستفاده مجرمانه از اینترنت با چه دشواری‌هایی روبه‌رو هستند؟
۲- جامعه جهانی چه مواردی را به‌عنوان جرم‌های سایبری که نیاز به بررسی دارند؛ می‌پذیرد؟
۳- برخی از جرم‌های جدید که از اینترنت ناشی می‌شوند، کدامند؟
۴- تعدادی از مجازات جرم‌های اینترنتی را توضیح دهید.

فصل پنجم

مسائلی که با دنیای آفلاین هم‌پوشانی دارند

هدف این بخش افزایش آگاهی از هم‌پوشانی اینترنت با دنیای آفلاین در نقاط کلیدی دولت، اقتصاد و محتوای آن‌هاست. افزایش آگاهی از نیاز به یک واکنش کنترلی مناسب نیز هدف بعدی است.

اینترنت روی دنیای آفلاین تأثیر می‌گذارد. آیا دنیای آفلاین باید اصلاح شود تا شباهت بیشتری به دنیای آنلاین پیدا کند؟ یا قوانین آفلاین باید در دنیای آنلاین استفاده شوند؟ قاعدتاً پاسخ در جایی بین این دو نهفته است.

۵-۱ سیاست رقابت

تا آن‌جا که امکان دارد، دسترسی به اینترنت باید رقابتی[1] باشد؛ یعنی بخش مخابرات[2] باید آزاد شود، به ویژه اگر این بخش انحصاری باشد. آزاد کردن این بخش برای بهبود کیفیت خدمات پیشنهاد داده شده است؛ در حالی که قیمت‌ها نیز کاهش یافته‌اند. قیمت‌گذاری پایین برای افزایش نفوذ اینترنت به کار رفته است و در مورد باند پهن[3]، قیمت‌گذاری پایین‌تر الگوی استفاده از اینترنت را تغییر می‌دهد. نظریه بازی[4] می‌گوید هر بازی باید حداقل سه بازیکن برای داشتن رقابت اثربخش داشته باشد.

آزاد کردن مخابرات و هزینه استفاده از اینترنت

گفته شده که دلیل ظهور اینترنت در ایالات متحده آزاد کردن بخش مخابرات است. اینترنت بیشتر از هر چیزی به مخابرات با مسافت طولانی بستگی دارد. رقابت در آن بخش قیمت‌ها را پایین می‌آورد. تأثیر آزاد کردن بیشتر در ایالات متحده آمریکا که آغازگر حرکت آزاد کردن مخابرات بود؛ آشکار است: در ایالات متحده آمریکا میزبانی[5]

1- Competitive
2- Liberalization of the Telecommunications Sector
3- Broadband
4- Game Theory
5- Host

یک وب سایت از اغلب کشورهای دیگر ارزان‌تر است. این مسئله هنگامی که صرفه‌جویی به واسطه افزایش حجم تولید[۱] باعث پایین ماندن قیمت‌ها می‌شوند، منجر به یک چرخه مفید[۲] خواهد شد.
تحقیقات نشان داده است که تقاضای مخابرات نسبتاً انعطاف‌پذیر است؛ یعنی افت قیمت X درصدی، منجر به افزایش استفاده بیشتر از X درصد می‌شود. مطالعات نشان داده‌اند که ایجاد رقابت در یک حلقه محلی[۳] مخابرات، منجر به نفوذ بیشتر در اینترنت می‌شود.
فرانسه، ژاپن و جمهوری کره از طریق سیاست‌های موافق رقابت[۴]، نفوذ باند پهن را افزایش داده‌اند. جمهوری کره بیشترین نفوذ باند پهن را در جهان دارد که باعث ورود آزاد به بخش مخابرات مبتنی بر امکانات[۵] از دهه ۱۹۸۰ شده است. نمونه‌های فرانسه و ژاپن آموزنده‌تر هستند، زیرا نرخ نفوذ آن‌ها تا سال ۲۰۰۵ زیاد بالا نبوده است. از آن پس سیاست‌های موافق رقابت، قیمت‌ها را کاهش و نفوذ باند پهن را افزایش داده‌اند.
از اواسط دهه ۱۹۸۰ تا اواسط دهه ۱۹۹۰، بسیاری از کتب و مقالات درباره مزایای آزاد کردن بخش مخابرات بحث می‌کنند. آزاد کردن بخش اینترنت، گسترش ایده‌های کشف شده در بخش مخابرات است. به امانوئل جیووانتی[۶]، «انقلاب فناوری اطلاعات، اینترنت و مخابرات: حرکت به سمت صنعت رقابتی در اتحادیه اروپا»، در *انقلاب اینترنت: یک چشم‌انداز جهانی*، ای. جیووانتی، ام. کاگامی[۷] و ام. سوجی[۸] رجوع کنید (مطبوعات دانشگاه کمبریج، ۲۰۰۳)، صفحه ۱۲۴ تا ۱۴۲.

۵-۲ سانسور و آزادی بیان

سانسور[۹] توسط دولت و بخش خصوصی در سراسر دنیا وجود دارد. همان‌طور که قبلاً بحث شد، مسئله ایجاد تعادل بین سلایق محلی و هنجار بین‌المللی اعمال سانسور کم یا عدم سانسور اینترنت است. مسدود کردن سایت‌های موردپسند جامعه اینترنتی نیست. عملی‌ترین و مقبول‌ترین راه‌حل تا حدودی در اصل فیلتر توسط کاربر[۱۰] قرار گرفته است. نرم‌افزارهای فیلتری که توسط کاربر نصب می‌شوند مورد قبول همگان هستند؛ اما مشخص شده است که والدین اغلب در نصب و استفاده از فیلترها مهارت فرزندان خود را ندارند.

1- Scale Economies
2- Virtuous Cycle
3- Local Loop
4- Pro-Competition Policies
5- Facility-Based
6- Emanuele Giovannetti
7- M. Kagami
8- M. Tsuji
9- Censorship
10- Filtering by the User

فیلتر داوطلبانه خود ارزیابی

در سال ۱۹۹۹، بنیاد برترسلمن[1] تیمی برای توسعه سیستم فیلتر محتوای اینترنت تشکیل داد که آزاد و حساس به فرهنگ بود و به حقوق آزادی بیان تجاوز نمی‌کرد. این تیم شامل محققان، قانون‌گذاران و هم‌چنین حامیان[2] آزادی بیان بود. نتیجه نهایی، تشکیل انجمن رتبه‌بندی محتوای اینترنت (ICRA)[3] بود.

گروه، نتیجه مطلوب را می‌دانست: والدین روی نام کشور خود کلیک می‌کنند، سپس روی یک سیستم فیلتر کلیک می‌کنند (یکی از آن‌ها توسط کلیسای کاتولیک[4] راه‌اندازی شد) و سپس سایت‌های نامناسب فیلتر می‌شوند. تحت سیستم فیلتر، سایت‌ها خود را برحسب زبان، خشونت و برهنگی و محتوای قابل اعتراض (نه غیر قانونی) مانند الکل طبقه‌بندی می‌کنند. روی هم رفته ۴۰ طبقه وجود دارد.

با این وجود، در پایان انجمن رتبه‌بندی محتوای اینترنت به هدف غایی خود نرسید. اولاً از طرف آزادی خواهان مدنی مانند مرکز دموکراسی و فناوری در ایالات متحده مورد مخالفت قرار گرفت. سایت‌های خبری که در ابتدا با خود–طبقه‌بندی موافق بودند، هنگامی که احساس کردند به آن‌ها به عنوان کسانی که در برابر سیستم سانسور تسلیم شده‌اند نگاه خواهد شد نظر خود را تغییر دادند. دوماً، برای تطبیق با مسائل آزادی بیان، وب سایت‌ها باید خودشان را طبقه‌بندی کنند. این عوامل توسعه تعدادی مکفی از وب سایت‌ها[5]یی را که خود را طبقه‌بندی می‌کنند، به تأخیر می‌اندازد. بدون توده حساس وب سایت‌ها، کاربران فیلتر مجبورند استفاده از فیلترها را تقریباً متوقف کنند. سوماً بهترین فیلترها درون مرورگرها قرار گرفته‌اند. زمانی که روش انجمن رتبه‌بندی محتوای اینترنت آماده اجرا بود، جنگ مرورگر[6] پایان یافت و مایکروسافت برنده شد. از آن به بعد، Netscape و مایکروسافت خصوصیاتی به مرورگرهای خود اضافه کردند. در حقیقت، مرورگر Microsoft 2000 یک سیستم فیلتر زمخت داشت. در نهایت، همان‌گونه که در دیگر سیستم‌های طبقه‌بندی مشابه مانند V-chip در ایالات متحده آمریکا که قرار بود محتوای خشن تلویزیون فیلتر شود؛ تجربه شده بود، تقاضای واقعی از طرف مصرف‌کنندگان وجود نداشت یا مصرف‌کنندگان به توافق شفاهی خود درباره نیاز به چنین طرح فیلتری عمل نکردند.

در سال ۲۰۰۷، انجمن رتبه‌بندی محتوای اینترنت به مؤسسه امنیت آنلاین خانواده[7] تبدیل شد.

از آنجایی که نویسنده عضو هیأت مدیره انجمن رتبه‌بندی محتوای اینترنت است، موارد بالا برای اولین بار به تفصیل بازگو می‌شوند. کتاب *نظم دادن به بی‌نظمی*[8] جزییاتی درباره انجمن رتبه‌بندی محتوای اینترنت در فصل «سانسور و تنظیم محتوای اینترنت»[9] آورده است.

1- Bertelsmann
2- Advocates
3- Internet Content Rating Association
4- Catholic Church
5- Critical Mass of Websites
6- Browser war
7- Family Online Safety Institute
8- Ordering Chaos
9- Censorship and Content Regulation of the Internet

رویکرد دیگر نصب فیلترهای سطح سرور[۱] هستند که به عنوان یک سرویس ارزش افزوده[۲] ویژه به کاربران فروخته می‌شوند. برای به‌روزرسانی و نگهداری لیست سایت‌های مسدود شده مبلغی پرداخت می‌شود. در این نوع فیلتر ورود برای یک کاربر متوسط غیر ممکن است. با این وجود عیب آن این است که برخی مواقع انسداد بیش از حد اتفاق می‌افتد و «عدم انسداد»[۳] سایتی که به اشتباه مسدود شده است مسئله است.

فعالیت

۱- مراحل کنترل محتوا را در کشور خود (در صورت وجود) شرح دهید.
۲- اگر دولت کشور دیگر از کشور شما بخواهد یک سایت را به این دلیل که محتوای آن در کشور آن‌ها غیر قانونی است مسدود کند، دولت شما چه اقدامی انجام خواهد داد؟ برای نظریه خود دلیل بیاورید.

۵-۳ توهین

با افزایش آزادی بیان در اینترنت فرصت فوق‌العاده‌ای برای توهین[۴] آنلاین به وجود می‌آید. به‌طور کلی، پرداختن به رسوایی نیاز به تعادل بین منافع مورد رقابت دارد: علاقه افراد به شهرت و علاقه اجتماعی در تشویق به آزادی بیان بیشتر. در اینترنت، پیچیدگی بیشتری در ارزش‌های فرهنگی متعارض و علایق اجتماعی و فردی نیز وجود دارد.

یکی از نمونه‌های آموزنده جوزف گوت‌نیک[۵]؛ تاجری از ملبورن استرالیاست. مجله بارون[۶] شرکت داو جونز[۷] آقای گوت‌نیک[۸] را در یک مقاله بدنام کرد. مجله ۱۴ مشترک[۹] در استرالیا داشت و ۵ نفر از آن‌ها در ایالت ویکتوریا بودند که برای اثبات دادرسی در دیوان عالی استرالیا[۱۰] کافی بود.[۵۳] بارون، ۱۷۰۰ مشترک آنلاین داشت که با کارت اعتباری استرالیایی پرداخت می‌کردند. این سؤال به وجود آمد: اگر گوت‌نیک دعوی را ببرد، آیا به این معنی است که کلیه ناشران باید آنچه را که با استفاده از شدیدترین قوانین توهین در کشور منتشر کرده‌اند، تماشا کنند؟ خوشبختانه، دیوان عالی تصمیم

1- Server-Level Filters
2- Value-Added Service
3- Un-Block
4- Defamation
5- Joseph Gutnick
6- Barron's
7- Dow Jones
8- Gutnick
9- Subscribers
10- Australian High Court

گرفت که خسارت مالی را که آقای گوت‌نیک می‌توانست مطالبه کند، خدشه‌دار کردن شهرت او در ملبورن، نه در سطح جهان تعیین کند.[۵۴] دیوان وانمود کرد که خسارت واقعی وارد شده از طرف مقاله توهین‌آمیز را در نظر گرفته است، چیزی که دادگاه‌های کشورهای مشترک‌المنافع[1] مایل به انجام آن نبودند.

فعالیت

شهروند Y را در کشور خود در موقعیت‌های زیر راهنمایی کنید:

موقعیت (۱):
وبلاگ W در کشور شما به Y توهین می‌کند. شهرت یا عدم شهرت وبلاگ اهمیت دارد؟ اگر ۲۰۰ پست از Y پشتیبانی کنند، تکلیف چیست؟

موقعیت (۲):
اگر سازمان اخبار آنلاین در ایالات متحده به شرکت Y توهین کند، تکلیف چیست؟ آیا باید «مسئولیت جهانی»[2] برای توهین اینترنتی در نظر گرفته شود؟

اینترنت تغییر دیگری در قوانین اینترنتی ایجاد کرده است: نیاز به یک ماده مصونیت[3] برای محتوای شخص ثالث. اگر میزبان‌های وب سایت و مجمع «معقولانه»[4] اقدام کنند؛ یعنی نسبت به محتوای توهین میز اخطار بدهند؛ مسئول محتوای پست شده توسط دیگران نیستند. در اکثر محکمه‌ها «اقدام معقول»[5] یعنی حذف محتوای توهین‌آمیز در طول تعداد روزهای مشخص.[۵۵] این مسئله ماده اخطار بده و کنار بکش[6] نیز نامیده می‌شود.

1- Commonwealth
2- Global Liability
3- Immunity Provision
4- Reasonably
5- Acting Reasonably
6- Notice-and-Take-Down Provision

٤-٥ کپی‌رایت و حقوق دیگر دارایی فکری

شکل ۱-۵ ایجاد تعادل در کپی‌رایت

منبع: DiploFoundation, http://textus.diplomacy.edu/textusbin/env/scripts/Pool/GetBin.asp?IDPool=1181.

یک حوزه بحث برانگیز بزرگ در حقوق دارایی فکری، در نظر گرفتن نام‌های حوزه به عنوان علامت تجاری است. شرکت‌های چند ملیتی[1]، مارک‌های بین‌المللی[2] و شخصیت‌های مشهور مایلند این دیدگاه را حفظ کنند که نام آن‌ها باید فقط توسط خودشان به عنوان نام حوزه استفاده شود. در ایالات متحده آمریکا؛ جایی که سرچشمه بسیاری از مارک‌های بین‌المللی است؛ قانون مخالفت با ثبت اینترنتی در پشتیبانی از مصرف‌کننده (ACPA)[3] مربوط به سال ۱۹۹۹ برای چنین شرکت‌ها یا افرادی کنترل آن دسته از نام‌های حوزه که بسیار شبیه نام یا مارک تجاری آن‌هاست بخصوص اگر مالک نام حوزه رفتار نادرستی داشته باشد، آسان‌تر می‌کند. با این وجود، بیشتر کشورهای دیگر چنین قانونی ندارند. بسیاری از کشورها مانند استرالیا و کانادا در سطح ccLTD بررسی می‌کنند که آیا ثبت‌کننده ارتباطی با نام حوزه ثبت شده دارد یا خیر. هنگامی که اختلافی به وجود آید اولویت با فرآیند یکسان حل اختلاف (UDRP)[4] است که توسط ICANN ایجاد شد، زیرا ارزان‌تر از استفاده از دادگاه‌هاست؛ اما دادگاه‌های ایالات متحده با استفاده از ACPA می‌توانند نتیجه‌ای بهتر از فرآیند یکسان حل اختلاف بگیرند.[۵۶] در عوض این مسئله منجر به «ربودن حوزه رزروشده»[5] شد که در آن معمولاً شرکت‌های بزرگ‌تر تلاش می‌کنند نام‌های حوزه مالکان را با کذب خواندن ادعای رفتار نادرست بگیرند.[۵۷]

مرکز وساطت و داوری سازمان مالکیت فکری جهانی (WIPO) که یک دستورالعمل برای مدیریت اختلافات نام حوزه براساس فرآیند یکسان حل اختلاف دارد؛ در سال ۲۰۱۰ گزارش داد که ۲۶۹۶ نمونه ثبت اینترنتی وجود داشته است.[۵۸] با شروع فعالیت حوزه‌های عمومی سطح بالای جدید؛ انتظار می‌رود تعداد شکایات افزایش یابد.

اکثر اختلافات اخیر مربوط به مسئولیت واسطه‌های[6] اینترنتی است. وب سایت‌هایی که به کاربران اجازه می‌دهند تا نظرات و توضیحاتی را پست کنند، ممکن است محتوایی دریافت کنند که کپی‌رایت و قوانین مدنی دیگر را نقض کند. تحت قانون متعارف چنین وب سایت‌هایی معمولاً مسئول تخلف هستند؛ حتی اگر خودشان محتوا را تولید نکرده باشند. از اواسط دهه ۱۹۹۰، قوانین به قدری اصلاح شدند که واسطه‌ها از برخی از فرم‌های مصونیت از مسئولیتی که «معقولانه» پاسخ می‌دادند برخوردار شدند.[۵۹] با این وجود، توافق‌نامه مخالفت با تقلب در تجارت (ACTA)[7] که در آوریل ۲۰۱۱ نهایی شد؛ در جهت مخالف آن مسیر حرکت می‌کند.

1- Multinational Companies
2- International Brands
3- Anti-Cybersquatting Consumer Protection Act
4- Uniform Dispute Resolution Process
5- Reverse Domain Hijacking
6- Intermediaries
7- Anti-Counterfeiting Trade Agreement

توافق‌نامه مخالفت با تقلب در تجارت تصمیم داشت به دزدی محتوای دیجیتال بپردازد. با این وجود فرآیند و خروجی توافق‌نامه مخالفت با تقلب در تجارت به چند دلیل مورد انتقاد قرار گرفته است. گروهی از فرهیختگان برجسته، بیانیه‌ای مشترک در نقد توافق‌نامه مخالفت با تقلب در تجارت منتشر کردند.[۶۰] اول، اگرچه کشورهای مذاکره‌کننده اکثریت غریب به اتفاق حقوق جهانی دارایی فکری را بنیان‌گذاری کردند، اما گروه کوچکی از کشورها هستند: استرالیا، کانادا، اتحادیه اروپا، ژاپن، جمهوری کره، مکزیک، مراکش، نیوزیلند، سنگاپور، سوییس و ایالات متحده آمریکا. دوم، توافق تا زمان نهایی شدن به صورت محرمانه مورد مذاکره قرار می‌گیرد.[۶۱] به طور کلی، مباحث قانونی حقوق دارایی فکری باید به روشی شفاف و باز انجام شود، زیرا به تعادل در منافع رقابتی مانند پشتیبانی از مصرف‌کننده، رقابت کسب‌وکار، حریم خصوصی و آزادی بیان نیاز است. سوم، مواردی وجود دارد که مسئولیت نقض کپی‌رایت را به واسطه‌ها مانند ارائه‌دهندگان خدمات اینترنتی (ISPs)[1] می‌سپارد.[۶۲]

در زمان نوشتن در اواخر سپتامبر ۲۰۱۱، حتی برخی از کشورهایی که در مذاکرات شرکت داشتند توافق را قبول نکردند.[۶۳]

پرسش‌هایی برای تفکر

۱- آیا باید نام‌های حوزه به عنوان نشان تجاری استفاده شوند؟ چرا؟

۲- شما چگونه بین منافع کشور خود و مالکان کپی‌رایت که ممکن است از کشورهای توسعه یافته باشند؛ تعادل برقرار می‌کنید؟

۵-۵ حریم خصوصی

همان‌گونه که قبلاً گفته شد، قوانین حریم خصوصی در اینجا بررسی می‌شوند. سؤال این است: کدام مدل باید برای کنترل حریم خصوصی استفاده شود؟ اساساً دو مدل با الگوهای[2] کاملاً متفاوت وجود دارد. در مدل اتحادیه اروپا (EU)، حریم خصوصی جزء حقوق بشر[3] است. قابل خرید، فروش یا معامله نیست و شایسته قانون‌گذاری جامع[4] است. در مدل ایالات متحده (US)، حریم خصوصی یک حق قانونی[5] است که قابل توافق است. به عنوان مثال، یک فرد به جای آدرس پست الکترونیکی،

1- Internet Service Providers
2- Paradigms
3- Human Right
4- Comprehensive Legislation
5- Legal Right

می‌تواند برخی از اسناد را بخواند یا برخی از خدمات را داشته باشد. قانون‌گذاری در سراسر صنایع جامع نیست، ولی چند تکه شده است.

در اینترنت، هر دو الگو در اجرا و خروجی بسیار شبیه هستند. البته مدل اروپایی مجازات‌های بیشتری دارد که هزینه‌ها را افزایش می‌دهد.

هر سبکی که یک کشور انتخاب کند، تحت تأثیر فرهنگ و تاریخ آن کشور قرار خواهد گرفت. با این وجود، اگر دستورالعمل محافظت از داده[1] اجرا شود، مدل اروپایی پتانسیل پذیرش جهانی را دارد.

نگهداری از داده‌هایی که آنلاین جمع‌آوری می‌شوند، در برخی مواقع به صورت نامحدود؛ اهمیت فزاینده آن‌ها را نشان می‌دهد. به عنوان مثال موتور جست‌وجوی Google کلیه نتایج جست‌وجوی خود را از زمان آغاز به کار خود نگه داشته است. سایت‌های شبکه اجتماعی[2] برخی مواقع حذف محتوا را برای کاربران دشوار می‌کنند. مثال کلاسیک کاربران سایت شبکه اجتماعی هستند که بعد از قراردادن یک عکس خجالت‌آور از آن‌ها روی سایت، شغل‌های خود را از دست دادند. بیشترین نگرانی سایت‌های شبکه اجتماعی این است که اطلاعات افراد قابل ردیابی هستند. قوانین محافظت از داده می‌توانند جمع‌آوری و نگهداری داده را با قید یک سری شروط محدود کنند. پیشنهاد شده است که باید یک تاریخ انقضا[3] برای بارگذاری[4] اطلاعات روی اینترنت وجود داشته باشد.[۶۴]

پرسش‌هایی برای تفکر

۱- حریم خصوصی در کشور شما تا چه حد به عنوان تقاضای قانونی کاربر شناخته می‌شود؟

۲- آیا کشور شما از مدل EU یا مدل US در قانون‌گذاری حریم خصوصی استفاده می‌کند؟ چرا این‌طور فکر می‌کنید؟

جمع‌بندی:

فرآیند قانون‌گذاری باید شفاف، دارای چندین ذی‌نفع و مردمی باشد. به همین دلیل فرآیند باید مشورتی[5] باشد تا کلیه ذی‌نفعان در آن شرکت کنند. قانون‌گذاری باید هر چهار سبک- بازار، هنجارهای اجتماعی، معماری و قانون‌گذاری دولتی (به انضمام خودکنترلی، برای اثربخشی خودکنترلی نیاز به قدرت محول شده از طرف دولت دارد) را کاوش کند.

1- Data Protection Directive
2- Social Network
3- Expiration Date
4- Upload
5- Consultive

خودآزمایی

۱- ارتباط بین سیاست رقابتی با دسترسی به اینترنت چیست؟
۲- سانسور اینترنت؛ در صورت وجود؛ تا چه حد قابل تحمل است؟
۳- آیا یک کاربر اینترنت می‌تواند فرد دیگری را به صورت آنلاین بدنام و سپس فرار کند؟
۴- آیا قانون توهین باید برای انطباق با اینترنت اصلاح شود؟
۵- چهار مسئله اصلی بحث‌برانگیز مربوط به کپی‌رایت و دیگر حقوق دارایی فکری در اینترنت کدامند؟
۶- دو رویکرد حریم خصوصی و محافظت از داده کدامند و چه تفاوت‌هایی دارند؟

فصل ششم

بعد توسعه: شکاف دیجیتال

این بخش شرح می‌دهد که چگونه اینترنت می‌تواند برای توسعه اجتماعی و اقتصادی؛ به اندازه محدودیت‌های توسعه به کمک فناوری اطلاعات و ارتباطات؛ استفاده شود.

توسعه ملی یکی از محرک‌های مجمع جهانی در مورد جامعه اطلاعاتی بود که سرانجام منجر به مناظره درباره نظارت بر اینترنت شد. با این وجود، توسعه مسئله بزرگی است که قرن‌های زیادی مورد بررسی قرار خواهد گرفت. امید فناوری‌های اطلاعاتی و ارتباطاتی این است که به تسریع فرآیند توسعه کمک خواهند کرد.

۱-۶ توسعه به کمک فناوری اطلاعات و ارتباطات

توسعه به کمک فناوری اطلاعات و ارتباطات برای اثربخشی باید موارد زیر را در برگیرد: (۱) نظارت و تفویض اختیار[1]، (۲) زیرساخت[2]، (۳) توسعه اقتصادی و (۴) توسعه اجتماعی. بدون نظارت مناسب، سرمایه‌ها هدر می‌رود. بدون تفویض اختیار، کاربران احساس نمی‌کنند که می‌توانند موقعیت خود را تغییر دهند. بدون زیرساخت مانند خطوط مخابراتی یا برق، پایداری اینترنت غیرممکن می‌شود.

مجمع جهانی در مورد جامعه اطلاعاتی به تأسیس سرمایه مشترک دیجیتال[3] کمک کرده است. اهداف توسعه هزاره راهنمایی مناسب برای خرج کردن سرمایه هستند. اهداف توسعه هزاره عبارتند از:

۱- ریشه‌کنی فقر و گرسنگی شدید
۲- کسب تحصیلات ابتدایی در سطح جهان
۳- ایجاد تساوی جنسیتی[4] و قدرت دادن به زنان
۴- کاهش مرگ و میر کودکان

1- Empowerment
2- Infrastructure
3- Digital Solidarity Fund
4- Gender Equality

۵- بهبود سلامت مادران
۶- مبارزه با ایدز[1]، مالاریا و بیماری‌های دیگر
۷- اطمینان از ثبات محیط
۸- ایجاد مشارکت جهانی[2] در توسعه

در مجموعه ماژول‌های *آکادمی اصول فناوری اطلاعات و ارتباطات برای مدیران ارشد دولتی*، ماژول ۱ درباره اتصال بین فناوری‌های اطلاعاتی و ارتباطاتی و اهداف توسعه هزاره بحث می‌کند.

اینترنت برای روستا

اینترنت به‌عنوان یک فناوری قدرتمند و مدرن، پتانسیل افزایش عدم‌تساوی درآمد بین افرادی را که از آن استفاده می‌کنند و افرادی که استفاده نمی‌کنند، دارد. یکی از چشم‌گیرترین نمونه‌های اختلاف ممکن است در هند یافت شود. در آنجا، جدیدترین فناوری‌ها را در شهرهای بزرگ می‌توان یافت؛ اما در مناطق روستایی هند مکان‌هایی وجود دارند که هندی‌ها آنجا را «تاریکی رسانه‌ها»[3] می‌نامند، جایی که تلویزیون نیز وجود ندارد.

برای گسترش کاربرد اینترنت و بررسی برخی از معضلات اجتماعی[4]، دولت هندوستان در سال ۲۰۰۷ یک پروژه ملی نظارت بر اینترنت به نام طرح مرکز خدمات مشترک (CSC)[5] راه‌اندازی کرد که در آن ۶۰۰,۰۰۰ روستا در هند ۱۰۰۰۰۰ مرکز اشتراکی خواهند داشت. اساساً این مراکز کیوسک‌های اینترنت[6] هستند.

سابقاً کیوسک‌های اینترنت موفقیت زیادی نداشتند. در حقیقت، اولین موج چنین کیوسک‌هایی فقط ۳ درصد موفقیت داشت. موفقیت در این مورد بعد از یک سال اندازه‌گیری شد. با استفاده از تجربه حاصل از اولین موج، دومین موج نرخ موفقیت ۳۰ درصدی داشت. ولی با وجود ۱۰ برابر افزایش، هنوز ۷۰ درصد نرخ شکست داشت. طرح مرکز خدمات مشترک موج سوم بود. این طرح بر اساس آخرین تحقیقات درباره برنامه‌های کاربردی مفید برای روستاها به‌طوری‌که زندگی آن‌ها را متحول سازد، راه‌اندازی شد.

به‌عنوان مثال، دولت هندوستان اجازه دسترسی به اسناد زمین[7] را داد، زیرا برخی مواقع مقامات رسمی در روستاها روستاییان را درباره زمین‌هایشان فریب می‌دادند. رایت CD[8] و چاپ عکس دیجیتال نیز دو روش تولید درآمد بودند. در شهر چنای[9] یک ابتکار خصوصی[10] نشان داد که قرار دادن اوراق امتحانی به‌صورت آنلاین دگرگون‌کننده است: نرخ قبولی روستاییان در امتحانات بزرگ پایین است؛ اما وقتی آنان با اوراق امتحانی آنلاین آزمون می‌دهند، نرخ قبولی بالا می‌رود. اطمینانی که با قبولی در امتحان حاصل می‌شود قدرت‌دهنده است.

1- HIV/AIDS
2- Global Partnership
3- Media Dark
4- Social Ills
5- Common Services Centre Scheme
6- Internet Kiosks
7- Land Titles
8- CD-Burning
9- Chennai
10- Private Initiative

طرح مرکز خدمات مشترک یک ایده ابتکاری است. علاوه بر استفاده از اینترنت برای حل مسائل اجتماعی (مانند تصرف غیرقانونی زمین) و محدود کردن شکاف دیجیتال، روی توسعه برخی مشاغل نیز هدف‌گذاری کرده است. اپراتورهای کیوسک‌های اینترنت در روستاها تبدیل به کارآفرینان بخش خصوصی[1] می‌شوند. در تئوری، این مطلب به این معنی است که هزینه دولت ملی پایین خواهد آمد، در حالی که انتظار می‌رود دولت‌های ایالتی پشتیبانی مالی داشته باشند درگیری بخش خصوصی سرمایه مالی را افزایش خواهد داد.

طرح اجرا شد. از تاریخ ۳۰ سپتامبر ۲۰۱۱، مجموعاً ۹۶,۷۳۳ مرکز خدمات مشترک در ۳۳ ایالت راه‌اندازی شدند.[۶۵] یعنی هدف ۱۰۰,۰۰۰ مرکز خدمات مشترک در ژوئن ۲۰۱۱ محقق نشد. حوزه فناوری اطلاعات[2] که سرپرست پروژه بود؛ کتابچه‌ای[3] منتشر کرد که حاوی داستان‌های موفقیت کارفرمایان روستایی با درآمد معمول تا عالی بین ۵,۰۰۰ روپیه[4] (۱۰۰ دلار آمریکا) و ۲۵,۰۰۰ روپیه (۵۰۰ دلار آمریکا) در هر مرکز بود.

برای اطلاعات بیشتر «طرح مرکز خدمات مشترک» حوزه فناوری اطلاعات، دولت هندوستان، http://www.csc-india.org را ببینید.

۲-۶ محدودیت‌ها و موانع

در این مرحله، باید به یاد داشته باشید که محدودیت‌هایی در استفاده از توسعه به کمک فناوری اطلاعات و ارتباطات وجود دارد. به‌عنوان مثال، استفاده از توسعه به کمک فناوری اطلاعات و ارتباطات فرض می‌کند که «اطلاعات بهتر به معنی تصمیمات بهتر» است که لزوماً مسئله اصلی نیست. هم‌چنین، بسیاری از برنامه‌های کاربردی فناوری اطلاعات و ارتباطات ابزاری برای توسعه یا پردازش اطلاعات هستند، نه ابزار ارتباطی؛ در حالی که ارتباطات اغلب منجر به نتایج مفیدی در توسعه می‌شوند. هم‌چنین موانعی برای کنترل افراد وجود دارد. زبان ممکن است یک مانع باشد. فساد[5] نیز یک مانع است.

هزینه هنوز یک مسئله اصلی است. با این وجود، هزینه‌ها ممکن است کاهش یابند. اولاً، دسترسی فزاینده به نرم‌افزار ارزان‌تر وجود دارد. دوماً دسترسی به نرم‌افزار با جنبش نرم‌افزار منبع باز و رایگان (FOSS)[6] امکان‌پذیر می‌شود. باید توجه داشت که برنامه‌های کاربردی نرم‌افزار منبع باز و رایگان ممکن است ارزان نباشند زیرا به نگهداری نیاز دارند و گهگاهی لازم است به برخی از بخش‌های دیگر برنامه نرم‌افزاری مانند چاپگر متصل شوند که ممکن است در دسترس نباشد و به‌صورت سفارشی نوشته شود.

1- Private Sector Entrepreneurs
2- Department of Information Technology
3- Booklet
4- INR
5- Corruption
6- Free and Open Source Software

۳-۶ برنامه‌های کاربردی توسعه به کمک فناوری اطلاعات و ارتباطات

برنامه‌های کاربردی مشهور و جاافتاده زیادی در زمینه توسعه به کمک فناوری اطلاعات و ارتباطات وجود دارد. همان‌طور که قبلاً شرح داده شد، اکثر آن‌ها برای ارائه اطلاعات هستند. چنین برنامه‌های کاربردی ممکن است در کشاورزی، آموزش و پرورش، خدمات بهداشتی و جهانگردی یافت شوند. غالباً این موضوع صحیح است که اطلاعات بهتر در این بخش‌ها منجر به خروجی بهتر می‌شود. به‌عنوان مثال، آگاهی از آنچه باید کشت شود به کشاورزان کمک می‌کند.

علاوه بر اطلاعات، ارتباطات مفیدتر نیز خواهد بود. به‌عنوان مثال، بعد از کشت آگاهی از مبارزه با آفاتی[1] که به گیاهان حمله می‌کنند مفید خواهد بود. با ایجاد ارتباطات بهتر، تحقق اهداف توسعه به کمک فناوری اطلاعات و ارتباطات محتمل‌تر می‌شود.

هدف ویژه توسعه و ارتقای خدمات دولت الکترونیکی[2] است. نمونه‌های خدمات دولت الکترونیکی شامل برنامه‌های کاربردی ویزا[3]، مالیات‌ها[4]، اسناد زمین، گواهینامه‌های رانندگی[5] و حتی ساده‌تر از این‌ها دسترسی به برنامه‌های کاربردی آنلاین است. برای شروع، ادارات دولتی باید کامپیوتری شوند. نتیجه کامپیوتری شدن[6] افزایش کارایی[7] دولت است. به‌عنوان مثال، آنلاین کردن مناقصات[8] دولتی باعث صرفه‌جویی مالی شده است. با کامپیوتری شدن، فرآیند شفاف‌تر و این خود باعث کاهش فساد می‌شود. کامپیوتری شدن هم‌چنین با ایجاد شغل فناوری اطلاعات[9] برای تکنیسین‌ها[10] و برنامه‌نویسان نرم‌افزار[11] موجب اقتصاد فناوری اطلاعات[12] می‌شود. کامپیوتری شدن به همراه استفاده از اینترنت، امکان مشورت بیشتر شهروندان را در مسائل عمومی مهم ایجاد می‌کند. این موضوع در عوض منجر به تفویض اختیار بیشتر به شهروندان می‌شود که شروعی در چرخه مفید توسعه است (در مجموعه ماژول‌های *آکادمی اصول فناوری اطلاعات و ارتباطات برای مدیران ارشد دولتی*، ماژول ۳ به بحث درباره برنامه‌های کاربردی دولت الکترونیکی می‌پردازد).

1- Combat the Pests
2- E-Government Services
3- Visa Applications
4- Taxes
5- Driving Licences
6- Computerization
7- Efficiency
8- Tenders
9- IT Career
10- Technicians
11- Software Programmers
12- IT Economy

گفته می‌شود که شفافیت بیشتر حاصل از خدمات دولت الکترونیکی، اغلب منجر به دموکراسی بیشتر می‌شود؛ اما مسئله اصلی این نیست. در حقیقت، خدمات دولت الکترونیکی کنترل بیشتر دولت مرکزی را امکان‌پذیر می‌کند. این مسئله آگاهی از سرانجام پایان ارائه خدمات را برای دولت مرکزی آسان‌تر می‌کند؛ بنابراین، در سطح محلی خدمات دولت پاسخ‌گوتر می‌شوند و در نتیجه فساد کاهش می‌یابد.[۶۶]

جمع‌بندی:

توسعه یکی از محرک‌های مجمع جهانی در مورد جامعه اطلاعاتی بود که منجر به شکل‌گیری کارگروه نظارت بر اینترنت شد؛ اما توجه زیادی به توسعه در گزارش نهایی کارگروه نظارت بر اینترنت نشد و اغلب در مناظرات نظارت بر اینترنت از آن چشم‌پوشی شد. جامعه بین‌المللی قطعاً می‌تواند با روش پروژه‌های سرمایه‌گذاری روی توسعه به کمک فناوری اطلاعات و ارتباطات کارهای زیادی انجام دهد. مشارکت عمومی–خصوصی (PPP)[1] با افزایش احتمال موفقیت پروژه‌ها روش پایدارتری در سرمایه‌گذاری ایجاد می‌کند (استفاده از مشارکت عمومی–خصوصی برای سرمایه‌گذاری در پروژه‌های توسعه به کمک فناوری اطلاعات و ارتباطات در ماژول ۸ از مجموعه ماژول‌های *آکادمی اصول فناوری اطلاعات و ارتباطات برای مدیران ارشد دولتی* بحث شده است)؛ اما بیشتر از آن دولت‌های ملی می‌توانند و باید از توسعه به کمک فناوری اطلاعات و ارتباطات استفاده کنند. هزینه دسترسی به نیازها باید کاهش یابد. به‌عنوان مثال، هزینه ثبت یک نام حوزه قابل کاهش است. سپس نیازها برای سیاسی شدن احتیاج به محیط قانونی دارند که موافق توسعه به کمک فناوری اطلاعات و ارتباطات باشد. استفاده از توسعه به کمک فناوری اطلاعات و ارتباطات به‌ویژه به‌عنوان ابزاری برای ارتباطات هرگز وعده داده نشده است.

خودآزمایی

۱- اینترنت چگونه می‌تواند در کسب اهداف توسعه کمک کند؟

۲- تعدادی از محدودیت‌ها و موانع استفاده از اینترنت در کسب اهداف توسعه را توضیح دهید.

1- Public-Private Partnership

فصل هفتم

نظارت بر اینترنت: نگاهی به جلو

این بخش مسائل برجسته نظارت بر اینترنت را شرح می‌دهد که مجمع نظارت بر اینترنت[1] نمی‌تواند و نمی‌خواهد حل کند و نیاز به توجه دولت دارد.

تعهد ۵ ساله مجمع نظارت بر اینترنت در سال ۲۰۱۰ خاتمه یافت. مزایای داشتن مجمع مشخص هستند. به‌طور مفهومی، مجمع فرصتی برای بحث درباره مسائل مهم و ایجاد آن مسائل در کشورهای کوچک‌تر به وجود آورد. در عمل باعث افزایش آگاهی از مسائل نظارت بر اینترنت شد و به بهبود درک اهمیت فرآیند نظارت بر اینترنت کمک کرد.

اکثر اقدامات نظارت بر اینترنت در نشست‌های موازی[2] انجام می‌شد که در آن‌ها برنامه‌ریزی به‌صورت غیرمتمرکز[3] توسط گروه‌های ارائه‌دهنده نشست‌ها انجام می‌شد. برخی از ائتلافات پویا[4] به‌ویژه در تعقیب منافع گروه‌های مربوط به خود فعال بوده‌اند. میزان موفقیت ائتلافات پویا متفاوت بوده است. به‌عنوان مثال، سازمان‌دهی جلسات نشست موازی هرزنامه بسیار فعال بود، اما بعد از آن متوقف شد.

مسائل موجود در گزارش نهایی کارگروه نظارت بر اینترنت پیچیده هستند و راه‌حل‌های آسان را نمی‌پذیرند. به‌عنوان مثال، مسئله سیاسی بینش بین‌المللی ICANN و DNS بارها به چاپ رسیده است. دولت ایالات متحده می‌تواند در شرایطی که ICANN هنوز در دستان اوست، ادعای «پیروزی»[5] داشته باشد. در پس‌زمینه این شکایت وجود دارد که با وجودی که حوزه‌های کد کشوری سطح بالا در دستان دولت‌های ملی است، اما به‌طور فیزیکی راهی برای متوقف کردن دولت ایالات متحده از حذف یک طرفه دولت‌ها در کنترل حوزه کد کشوری سطح بالای خود وجود ندارد. موانع عملی[6] وجود دارد اما هیچ مانع فیزیکی وجود ندارد، یعنی این امکان ضعیف هنوز هست که یک کشور از اینترنت حذف شود.

1- Internet Governance Forum
2- Parallel Sessions
3- Decentralized
4- Dynamic Coalitions
5- Victory
6- Practical Restraints

بخش‌های مهم دیگر- در استفاده از اینترنت، مسائل مربوط به اینترنت اما با تأثیر عمیق‌تر و توسعه جنبه‌های اینترنت- راه‌حل‌های آسان را نمی‌پذیرند. آنچه مجمع نظارت بر اینترنت می‌تواند انجام دهد کمک به مشخص کردن بهترین شیوه‌ها[1] برای حل آن‌هاست؛ بنابراین ایجاد ظرفیت برای نظارت بر اینترنت نیز مسئله‌ای همیشگی خواهد شد که همه دولت‌ها باید آن را بررسی کنند.

بحث درباره گزارش نهایی کارگروه نظارت بر اینترنت آگاهی از اهمیت مسائل نظارت بر اینترنت را افزایش داده است. از آنجایی که حل مسائل زمان‌بر است، دولت‌ها باید ظرفیت بررسی مسائل و شرکت در مناظره بین‌المللی درباره آن‌ها را ایجاد کنند. این ظرفیت‌سازی ضروری است، زیرا نظارت بر اینترنت فقط یک موضوع بین‌المللی نیست. توسعه به کمک فناوری اطلاعات و ارتباطات به مهم‌ترین موضوع دولت محلی تبدیل شده است و بسیاری از مسائل نظارت بر اینترنت، محلی هستند. به این دلیل، دولت‌های محلی و ملی نقش کلیدی در نظارت بر اینترنت بازی می‌کنند.

خلاصه

این ماژول نظارت بر اینترنت به بحث درباره مسائل زیر پرداخت:

نظارت بر اینترنت بیشتر درباره نظارت است تا اینترنت. مسائل سیاسی مربوط به سیاست بین‌المللی اینترنت، استفاده و سوءاستفاده از اینترنت و گسترش اینترنت برای کمک به توسعه اقتصادی و اجتماعی را پوشش می‌دهد.

برخلاف تصور عموم، اینترنت یک نقطه کنترل مرکزی[2] در ناحیه‌ای دارد که سیستم منطقه ریشه نامیده می‌شود. این سیستم منطقه مرکزی تحت کنترل یک نهاد دولتی در ایالات متحده به نام ICANN است.

کارگروه نظارت بر اینترنت توسط سازمان ملل برای حل تنش مربوط به بعد سیاسی نظارت بر اینترنت تأسیس شد. بعد از گزارش کارگروه نظارت بر اینترنت در معامله پایاپای[3] وجود یک مجمع ساده نظارت بر اینترنت باید موردقبول واقع شود، اما سیستم منطقه ریشه هنوز در دستان ICANN است با این شرط که فقط دولت‌های ملی می‌توانند حوزه‌های کد کشوری سطح بالای خود را کنترل و اداره کنند.

نظارت بر اینترنت باید چندجانبه و چندبخشی باشد. به همین دلیل هیچ کشور یا نهادی نباید به‌تنهایی اظهارنظر قطعی درباره نظارت بر اینترنت داشته باشد. در عوض، فرآیند چه در سطح ملی چه

1- Best Practices
2- Central Control Point
3- Horse-Trading

در سطح بین‌المللی باید مردمی باشد. در سطح بین‌المللی مشارکت در نظارت بر اینترنت باید در تمام کشورها، تمام سطوح و در بخش‌های خصوصی و جامعه مدنی گسترده باشد.

در زندگی دنیای آفلاین اینترنت ممکن است با چهار سبک تنظیم شود: قانون، هنجارهای اجتماعی، سازوکارهای بازار و معماری. از آنجایی که اجرای قانون در اینترنت همواره پایدار نیست، دولت‌ها باید در رویکردهای قانون‌گذاری اینترنت خلاق باشند.

خودکنترلی فرمی از قانون‌گذاری دولتی است. اغلب به‌عنوان یک فرم مقدم در قانون‌گذاری اینترنت توصیه می‌شود، اما محدودیت‌ها و هزینه‌هایی برای عملی کردن آن وجود دارد.

یک نقشه راهنما برای قانون‌گذاری اینترنت پیشنهاد شده است که انتشار آن را در حالی که معایبی نیز دارد تشویق می‌کند.

اینترنت روش‌های جدیدی برای برخی از رفتارهای مجرمانه قدیمی و جرائم جدیدی نیز ایجاد کرده است. یکی از مسائل اجرایی، تعریف جرم است.

دو ناحیه که در آن توافق جهانی وجود دارد، هرزه‌نگاری کودکان و کلاهبرداری از مصرف‌کننده است. آژانس‌های اجرایی برای پیگیری این جرائم مشارکت می‌کنند.

هرزنامه، اسکم، کد مخرب و فیشینگ به‌طورکلی جرم تلقی می‌شوند، اما برخی از کشورها قانونی علیه آن ندارند.

حتی در قانون‌گذاری و اقدام علیه مزاحمت سایبری، کمین سایبری، سرقت هویت و اعتیاد به اینترنت نیز توافق وجود ندارد.

فرم نظارت بر اینترنت جرقه ایجاد «اتحاد پویا»[1] را در جایی زده است که در آن گروه‌ها علاقه‌مند به پرداختن به یک مسئله خاص هستند و می‌توانند درباره بهترین شیوه‌ها و اقدامات معمول بحث کنند.

از آنجایی که قوانین باید خلاقانه باشند، مجازات اینترنتی نیز باید خلاقانه باشند.

در پایان، مشارکت بین‌المللی برای شکست رفتار مجرمانه در اینترنت ضروری است.

مسائل نظارت بر اینترنت در دنیای آفلاین پراکنده شده‌اند. نمونه‌ها شامل سیاست رقابت، سانسور و آزادی بیان، توهین، کپی‌رایت و حقوق دارایی فکری و حریم خصوصی است.

یکی از محرک‌های مطالعه نظارت بر اینترنت این نگرانی بود که کشورهای در حال توسعه در اقتصاد اطلاعات عقب می‌مانند؛ بنابراین استفاده از توسعه به کمک فناوری اطلاعات و ارتباطات بخش مهمی در نظارت بر اینترنت است.

در استفاده از توسعه به کمک فناوری اطلاعات و ارتباطات محدودیت‌ها و موانعی وجود دارد.

داستان‌های موفقیت نیز وجود دارند که عبرت‌آموز هستند.

1- Dynamic Alliances

توسعه به کمک فناوری اطلاعات و ارتباطات می‌تواند با بهبود مثلاً شفافیت به بهبود نظارت بر دنیای واقعی کمک کند.

تنش سیاسی در نظارت بر اینترنت حل نشده است و ایجاد ظرفیت برای نظارت بر اینترنت یک مسئله همیشگی باقی مانده است که تمام دولت‌ها باید به آن بپردازند.

مطالعات بیشتر

Ang, Peng Hwa. *Ordering Chaos: Regulating the Internet.* Singapore: Thomson, 2005.

Butt, Danny, ed. *Internet Governance: Asia-Pacific Perspectives*. Bangkok: UNDP-APDIP, 2005.

Available from http://www.apdip.net/publications/ict4d/igovperspectives.pdf.

Cukier, Kenneth Neil. Who Will Control the Internet? *Foreign Affairs*, (November/December

2005). Available from http://www.foreignaffairs.org/20051101fa comment8460 2/kenneth-neilcukier/

who-will-control-the-internet.html.

Drissel, David. Internet Governance in a Multipolar World: Challenging American Hegemony.

Cambridge Review of International Affairs, vol. 19, No.1, (March 2006), pp. 105-120.

Kapur, Akash. *Internet Governance: A Primer*. Bangkok: UNDP-APDIP, 2005. Available from

http://www.apdip.net/publications/iespprimers/eprimer-igov.pdf.

Working Group on Internet Governance. 2005. *Report of the Working Group on Internet Governance*. Available from http://www.wgig.org.

Wu, Tim, and others. On the Future of Internet Governance. *American Society of International Law*

Proceedings of the Annual Meeting, vol. 101. Available from http://ssrn.com/abstract=992805.

واژه‌نامه

آدرس پروتکل اینترنت **IP Address**

شناسه متناظر منحصربه‌فرد برای هر کامپیوتر یا یک ابزار در یک شبکه پروتکل اینترنت. در حال حاضر دو نوع آدرس IP قابل‌استفاده وجود دارند. IP نسخه ۴ (IPv4) و IP نسخه ۶ (IPv6). IPv4 (که از اعداد ۳۲ بیتی استفاده می‌کند) از سال ۱۹۸۳ استفاده شده است و هنوز متداول‌ترین نسخه است. اجرای پروتکل IPv6 در سال ۱۹۹۹ آغاز شد. آدرس‌های IPv6 اعداد ۱۲۸ بیتی هستند.

ثبت‌کننده **Registrar**

شخصی که توسط یک دفتر ثبت برای فروش/ثبت‌نام‌های حوزه تأیید («مجاز») شده است.

دفتر ثبت **Registry**

یک شرکت یا سازمان که از پایگاه‌های داده ثبت مرکزی برای نام‌های حوزه سطح بالا یا بلوک‌های آدرس IP نگهداری می‌کند (مثلاً RIR، به قسمت بعدی مراجعه کنید). برخی از دفاتر ثبت بدون ثبت‌کننده‌ها و برخی با ثبت‌کننده‌ها عمل می‌کنند، اما اجازه ثبت مستقیم از طریق دفتر ثبت را نیز می‌دهند.

دفاتر ثبت اینترنتی منطقه‌ای **RIRs**

این سازمان‌های غیرانتفاعی مسئول توزیع آدرس‌های IP در سطح منطقه‌ای به ارائه‌دهندگان خدمات اینترنت و دفاتر ثبت محلی هستند.

سرورهای ریشه **Root servers**

سرورهایی که شامل اشاره‌گرهایی به سرورهای نام معتبر برای کلیه حوزه‌های سطح بالا هستند. علاوه بر ۱۳ سرور ریشه اصیل که حامل فایل منطقه ریشه برای مدیریت شماره‌های اختصاصی اینترنت هستند، اکنون تعداد زیادی سرور یک به یک وجود دارد که اطلاعات یکسانی ارائه می‌دهند و توسط برخی از ۱۲ اپراتور اصلی در سطح جهان استقرار یافته‌اند.

فایل منطقه ریشه **Root zone file**

فایل اصلی که حاوی اشاره‌گرهایی به سرورهای نام برای کلیه حوزه‌های سطح بالاست.

WHOIS

یک پروتکل پرس‌وجو/پاسخ تراکنشی[1] است که به‌طور گسترده برای ارائه سرویس‌های اطلاعاتی به کاربران اینترنت استفاده می‌شود. در حالی که در ابتدا توسط اغلب (نه همه) اپراتورهای دفتر ثبت حوزه سطح بالا برای ارائه سرویس‌های «صفحات سفید»[2] و اطلاعاتی درباره نام‌های حوزه ثبت شده استفاده می‌شد، کاربرد اخیر محدوده بزرگ‌تری از سرویس‌های اطلاعاتی شامل جست‌وجوی RIR WHOIS برای اطلاعات تخصیص آدرس IP را پوشش می‌دهد.

1- Transaction Oriented Query/Response Protocol
2- White Pages

پیوست‌ها

نکاتی برای مربیان

همان‌گونه که در بخش «درباره مجموعه سرفصل‌ها» اشاره شد، این سرفصل و سرفصل‌های دیگر مجموعه جهت ایجاد ارزش برای مجموعه‌های مختلف مخاطبان و شرایط مختلف و متغیر ملی طراحی شده‌اند. این سرفصل‌ها هم‌چنین به سبک‌های مختلف به‌صورت کلی یا بخشی از آن‌ها، آنلاین یا آفلاین ارائه داده می‌شوند. سرفصل ممکن است توسط افراد یا گروه‌های آموزشی در مؤسسات و ادارات دولتی مورد مطالعه قرار گیرد. معلومات قبلی شرکت‌کنندگان و مدت جلسات آموزشی میزان جزییات را در ارائه محتوا تعیین خواهد کرد.

این «یادداشت‌ها» به مربیان ایده‌ها و پیشنهادهایی می‌دهد تا محتوای سرفصل را به‌طور اثربخش‌تر ارائه دهند. راهنمایی بیشتر در زمینه استراتژی‌ها و رویکردهای آموزشی در یک کتابچه راهنمای آموزشی به‌عنوان یک عنصر همراه در مجموعه سرفصل‌های *آکادمی اصول فناوری اطلاعات و ارتباطات برای مدیران ارشد دولتی* ارائه داده شده است. کتابچه راهنما در سایت http://www.unapcict.org/academy موجود است.

استفاده از سرفصل

هر بخش از سرفصل حاضر با شرحی از اهداف یادگیری آغاز و با مجموعه‌ای از پرسش‌های «خودآزمایی» پایان می‌یابد. خوانندگان می‌توانند از اهداف و پرسش‌ها به‌عنوان مبنایی برای ارزیابی پیشرفت خود در سرفصل استفاده کنند. هر بخش هم‌چنین شامل پرسش‌هایی برای بحث و تبادل و نظر و تمرینات عملی برای استفاده خوانندگان یا مربیان است. این پرسش‌ها و فعالیت‌ها طراحی شده تا به کاربران امکان داده شود از تجربه خود برای محک‌زنی محتوا و تفکر عمیق درباره مسائل ارائه شده استفاده کنند.

مطالعات موردی بخش مهمی از محتوای سرفصل هستند. هدف آن‌ها بحث و تحلیل، به‌ویژه برحسب میزان کارکرد مفاهیم کلیدی و اصول ارائه داده شده سرفصل در نمونه‌های واقعی است. در نمونه نظارت بر اینترنت، مسائل بین‌المللی و ملی یا محلی هستند. کار زیادی در سطوح محلی و ملی، بخصوص در استفاده از فناوری اطلاعات و ارتباطات؛ از جمله اینترنت؛ برای توسعه وجود دارد. مربیان می‌توانند شرکت‌کنندگان را تشویق به ارائه مثال‌ها و نمونه‌های مربوط به تجربیات خود کنند تا به بحث درباره سرفصل روحی تازه ببخشند.

ساختار جلسات

بسته به مخاطب، زمان و شرایط و تنظیمات محلی محتوای سرفصل می‌تواند در ظرف‌های زمانی ساخت‌یافته ارائه داده شود. ممکن است مقامات رسمی ارشد دولت نیاز به مقداری به‌روزرسانی و اطلاعات درباره نظارت بر اینترنت داشته باشند. بنابراین برنامه آموزشی باید جلسات کوتاه یک یا دو ساعته داشته باشد. برنامه کامل آموزشی حداقل یک و نیم روز زمان می‌برد. سرفصل سه جلسه اولیه شامل تاریخچه و تئوری و جلسات باقیمانده درباره برنامه کاربردی است.

برای جلسه یک یا دو ساعته

بخش‌های مختصر اول و دوم، روی مسائل و خروجی‌های اجلاس جهانی در مورد جامعه اطلاعاتی و کارگروه نظارت بر اینترنت تمرکز دارد. بخش ششم، توسعه به‌کمک فناوری اطلاعات و ارتباطات را شامل می‌شود.

برای جلسه سه ساعته

جلسات اول و دوم در بالا توضیح داده شد. بسته به شرکت‌کنندگان، بخش‌های سوم، چهارم، پنجم و ششم را با دیدگاه زیر ترکیب کنید:

یک چارچوب قانونی ایجاد کنید که در آن روی بخش‌های چهارم و پنجم تمرکز شود یا از توسعه به کمک فناوری اطلاعات و ارتباطات برای تمرکز روی بخش‌های پنجم و ششم استفاده کنید.

برای جلسه یک روزه (۶ ساعته)

فصل‌های اول، دوم و سوم را در صبح پوشش دهید. بعد از ظهر، با استفاده از فعالیت‌ها و پرسش‌هایی برای بحث فصل‌های چهارم، پنجم و ششم را بررسی کنید. باید بعد از ناهار انرژی خود را حفظ کنید. با فصل هفتم روز را خاتمه دهید.

برای جلسه یک و نیم روزه

اگرچه هفت فصل وجود دارد، اما مدت آن‌ها متفاوت است. شما باید نسبت به اهداف گروه و انتظارات آن‌ها از آموزش حساس باشید. معلومات قبلی فصل‌های اول و دوم سنگین است. اگر گروه علاقه‌مند به آن نباشد ولی خواهان خروجی باشد، پس روی خروجی تمرکز کنید. به‌طورکلی، احتمالاً شرکت‌کنندگان نیاز به مهارت‌های عملی بیشتری خواهند داشت. بحث‌ها و اشتراک اطلاعات باید مفید باشد تا آموزش را تقویت کند.

برای جلسه سه روزه

در روز اول درباره فصل‌های اول و دوم بحث کنید. بسته به چگونگی پاسخ‌دهی گروه، ممکن است بتوانید به فصل سوم بروید. در روز دوم، فصل‌های سوم، چهارم و پنجم را پوشش دهید. در روز سوم، درباره فصل‌های ششم و هفتم بحث کنید. سرعت حرکت اهمیت دارد. شرکت‌کنندگان باید تشویق به ارائه و اشتراک تجربیات خود در کلاس شوند. به‌ویژه، شرکت‌کنندگان باید تشویق به استفاده از فصل ششم برای پرداختن به مسئله شکاف دیجیتال در کشورهای خود شوند. فصل هفتم فرصتی برای به نتیجه رسیدن کل جلسه ایجاد می‌کند.

درباره مؤلف

آنگ پنگ هوا[1] پروفسور و رئیس مرکز تحقیقات اینترنتی سنگاپور در مدرسه اطلاعات و ارتباطات وی کیم وی[2]، دانشگاه فناوری نان‌یانگ[3] سنگاپور است. هم‌چنین در حال آموزش وکالت است و سیاست و قانون رسانه را تدریس می‌کند. تحقیق او در حوزه نظارت بر اینترنت است. کتاب سال ۲۰۰۵ او؛ *نظم دادن به بی‌نظمی: قانون‌گذاری اینترنت*؛ می‌گوید که اینترنت می‌تواند کنترل شود، کنترل می‌شود و باید کنترل شود.

او در سال ۲۰۰۴ توسط دبیر کل سازمان ملل برای کار گروهی در زمینه نظارت بر اینترنت جهت ایجاد گزارش برای جلسه اوج جهان در جامعه اطلاعاتی منصوب شد. او بعداً در تأسیس شبکه دانشگاهی جهانی نظارت بر اینترنت[4] کمک کرد و در آن مسئول افتتاحیه بود. او در حال حاضر به‌عنوان رئیس مرکز اطلاعات و ارتباطات رسانه آسیایی[5] کار می‌کند.

UN- APCICT/ESCAP

مرکز فناوری اطلاعات و ارتباطات توسعه آسیا و اقیانوسیه سازمان ملل (APCICT/ESCAP) بدنه اصلی گروه اجتماعی و اقتصادی سازمان ملل در آسیا و اقیانوسیه به شمار می‌رود (UN-ESCAP APCICT/ESCAP کمک می‌کند تا تلاش کشورهای عضو ESCAP در استفاده از فناوری اطلاعات و ارتباطات در توسعه اقتصادی – اجتماعی از طریق ایجاد ظرفیت‌های انسانی و سازمانی تقویت شوند و بر سه محور متمرکز است:

1- Ang Peng Hwa
2 -Wee Kim Wee
3- Nanyang
4- Global Internet Governance Academic Network
5- Asian Media Information and Communication Centre

۱- آموزش: افزایش دانش و مهارت‌های فناوری اطلاعات و ارتباطات سیاست‌گذاران و کارشناسان فناوری اطلاعات و ارتباطات و تقویت ظرفیت مربیان و مؤسسات آموزشی فناوری اطلاعات و ارتباطات.
۲- تحقیق: انجام مطالعات تحلیلی مربوط به توسعه منابع انسانی در فناوری اطلاعات و ارتباطات.
۳- مشاوره: ارائه خدمات مشاوره‌ای در زمینه برنامه‌های توسعه منابع انسانی به اعضای ESCAP.

UN.APCICT/ESCAP در اینچئون جمهوری کره واقع شده است.
http://www.unapcict.org

ESCAP

ESCAP بازوی توسعه منطقه‌ای سازمان ملل است و به‌عنوان مرکز اصلی توسعه اقتصادی و اجتماعی سازمان ملل در منطقه آسیا و اقیانوسیه خدمت می‌کند. دستور کارش ترویج همکاری بین ۵۳ عضو خود و نه عضو همراه است. ESCAP ارتباط استراتژیک بین برنامه‌ها و موضوعات کشوری و جهانی را ارائه می‌دهد و از دولت کشورهای منطقه و رویکردهای منطقه‌ای برای حل چالش‌های اقتصادی-اجتماعی منطقه‌ای در جهان حمایت می‌کند. اداره ESCAP در بانکوک تایلند واقع شده است.
http://www.unescap.org

آکادمی نیازمندی‌ها فناوری اطلاعات و ارتباطات برای رهبران دولتی

این آکادمی یک فناوری اطلاعات و ارتباطات فراگیر برای دوره آموزشی کامل با یازده سرفصل است که کمک می‌کند تا سیاست‌گذاری با دانش و مهارت‌های ضروری تجهیز شوند و بتوانند فرصت‌های ارائه شده از سوی فناوری‌های اطلاعاتی و ارتباطی دست‌یابی به اهداف توسعه و نفوذ و شکاف دیجیتالی را با ایجاد پل می‌کنند. در زیر توضیح کوتاهی از ده سرفصل این آکادمی آورده شده است:

سرفصل ۱- ارتباط بین کاربردهای فناوری اطلاعات و ارتباطات و توسعه هدفمند

مسائل کلیدی و نقاط تصمیم‌گیری، از خط‌مشی تا پیاده‌سازی در کاربرد فناوری‌های اطلاعاتی و ارتباطی در دسترسی به اهداف توسعه هزاره را متمایز می‌کند.

سرفصل ۲- فناوری اطلاعات و ارتباطات برای توسعه سیاست، فرآیند و حاکمیت فناوری اطلاعات و ارتباطات

بر سیاست‌گذاری و حاکمیت توسعه به‌کمک فناوری اطلاعات و ارتباطات تمرکز دارد و اطلاعات مهمی درباره جنبه‌های سیاست‌ها، استراتژی‌ها و چارچوب‌های ملی ارتقای توسعه به‌کمک فناوری اطلاعات و ارتباطات ارائه می‌دهد.

سرفصل ۳- کاربردهای دولت الکترونیکی

اصول و مفاهیم دولت الکترونیکی و نمونه‌هایی از برنامه‌های کاربردی را بررسی می‌کند. هم‌چنین به بحث پیرامون تهیه سامانه‌های دولت الکترونیکی و شناسایی ملاحظات طراحی می‌پردازد.

سرفصل ۴- روندهای فناوری اطلاعات و ارتباطات برای مدیران ارشد دولتی

نگرش‌هایی درباره روندهای جاری فناوری اطلاعات و ارتباطات و جهت‌گیری‌های آتی آن ارائه می‌دهد. هم‌چنین به ملاحظات کلیدی فنی و سیاسی هنگام تصمیم‌گیری برای توسعه به‌کمک فناوری اطلاعات و ارتباطات می‌نگرد.

سرفصل ۵- نظارت بر اینترنت

به بحث پیرامون توسعه سیاست‌ها و روال‌های بین‌الملل ناظر بر استفاده از اینترنت می‌پردازد.

سرفصل ۶- امنیت و محرمانگی اطلاعات

اطلاعاتی پیرامون مسائل و روندهای امنیتی و فرآیند تدوین استراتژی امنیت اطلاعات ارائه می‌دهد.

سرفصل ۷- مدیریت پروژه فناوری اطلاعات و ارتباطات در عمل و نظر

مفاهیم مدیریت پروژه‌های توسعه به‌کمک فناوری اطلاعات و ارتباطات شامل روش‌ها، فرآیندها و رشته‌های دانشگاهی مدیریت پروژه را معرفی می‌کند.

سرفصل ۸- گزینه‌های سرمایه‌گذاری توسعه به کمک فناوری اطلاعاتی و ارتباطی

گزینه‌های بودجه‌بندی برای پروژه‌های توسعه به‌کمک فناوری اطلاعات و ارتباطات و دولت الکترونیکی را بررسی می‌کند. به شراکت بخش‌های خصوصی و دولتی به‌عنوان گزینه بودجه‌بندی مفید در کشورهای درحال‌توسعه تأکید می‌کند.

سرفصل ۹- فناوری اطلاعات و ارتباطات برای مدیریت ریسک بلایا

مروری بر مدیریت ریسک بلایا و اطلاعات مورد نیازش دارد و درعین‌حال به شناسایی فناوری قابل‌دسترسی جهت کاهش ریسک بلایا و پاسخ به آن‌ها می‌پردازد.

سرفصل ۱۰- فناوری اطلاعات و ارتباطات، تغییرات اقلیمی و رشد سبز

نقش فناوری‌های اطلاعاتی و ارتباطی در مشاهده و پایش محیط، به اشتراک‌گذاری اطلاعات، اقدام به تجهیز، ترویج پایداری محیط زیست و کاهش تغییرات اقلیمی را نشان می‌دهد.

سرفصل ۱۱- توسعه به‌کمک رسانه اجتماعی

این سرفصل به معرفی مفهوم رسانه اجتماعی و کاربردهای متنوع آن در پیشرفت‌های اجتماعی و اقتصادی می‌پردازد. این سرفصل همچنین به هدایت خط‌مشی رسانه اجتماعی می‌پردازد.

این سرفصل‌ها با مطالعات موردی محلی توسط شرکای آکادمی ملی سفارشی‌سازی می‌شوند. شرکای آکادمی تضمین می‌کنند که این سرفصل‌ها مرتبط هستند و نیاز سیاست‌گذاران در کشورهای مختلف را برآورده می‌سازند. این سرفصل‌ها به زبان‌های مختلف ترجمه شده‌اند تا تضمین کنند که این برنامه مرتبط باقی می‌ماند و روندها را توسعه به‌کمک فناوری اطلاعات و ارتباطات بررسی می‌کند. APCICT به‌طور منظم این سرفصل‌ها را بازبینی و سرفصل‌های جدید را توسعه می‌دهد.

آکادمی مجازی APCICT

آکادمی مجازی APCICT بخشی از سازوکار ارائه چندکاناله است که در پیاده‌سازی برنامه ظرفیت‌سازی توسعه به‌کمک فناوری اطلاعات و ارتباطات آکادمی الزامات فناوری اطلاعات و ارتباطات برای سران دولتی به کار می‌رود.

این آکادمی به فراگیران امکان می‌دهد تا به دروس آنلاین دسترسی داشته باشند و دانش خود را در تعدادی از زمینه‌های مهم فناوری اطلاعات و ارتباطات از جمله بهره‌برداری از پتانسیل فناوری‌های اطلاعاتی و ارتباطی برای رسیدن به اجتماعات دورافتاده، افزایش دسترسی به اطلاعات، بهبود ارائه خدمات، ارتقای یادگیری در طول عمر و بالاخره ایجاد پل بین شکاف دیجیتالی و دسترسی به اهداف توسعه هزاره افزایش دهند.

تمام دروس آکادمی به‌صورت تدریس و آزمون مجازی و به‌سادگی قابل‌پیگیری هستند و به کاربران گواهینامه APCICT مشارکت در تکمیل موفق دروس اعطا می‌شود. تمام سرفصل‌ها به زبان انگلیسی هستند و نسخه‌های محلی شده به زبان روسی و Bahasa روی اینترنت قابل‌دسترس‌اند. به‌علاوه، طرح‌های توسعه بیشتر محتوا و بومی‌سازی بیشتر در دست اقدام هستند.

مرکز تشریک‌مساعی الکترونیکی

مرکز تشریک مساعی الکترونیکی پلت‌فرم آنلاین مختص APCICT برای به اشتراک گذاشتن روی توسعه به‌کمک فناوری اطلاعات و ارتباطات است و از طریق دسترسی آسان به منابع مرتبط و فضای اینترنت برای به اشتراک گذاشتن بهترین درس‌ها و تمرین‌های توسعه به‌کمک فناوری اطلاعات و ارتباطات به افزایش تجربه یادگیری و آموزش کمک می‌کند. این مرکز موارد زیر را ارائه می‌دهد:

- ✓ یک شبکه به اشتراک‌گذاری دانش و پورتال منابع برای توسعه به‌کمک فناوری اطلاعات و ارتباطات
- ✓ دسترسی آسان به منابع از طریق سرفصل
- ✓ فرصت بحث‌های آنلاین و تبدیل شدن به بخشی از جامعه تمرین آنلاین مرکز تشریک مساعی الکترونیکی که به اشتراک‌گذاری و توسعه دانش مبتنی بر توسعه به‌کمک فناوری اطلاعات و ارتباطات کمک می‌کند.

منابع

1- Peng Hwa Ang, Ordering Chaos: Regulating the Internet (Singapore, Thomson, 2005).
2- Katie Hafner and Mathew Lyon, Where Wizards Stay Up Late: The Origins of the Internet (New York, Simon and Schuster, 1998).
3- David S. Isenberg, “The Dawn of the Stupid Network”, ACM Networker 2.1, February/March 1998, pp. 24-31, http://www.isen.com/papers/Dawnstupid.html.
4- Any book that touches on the history of the Internet would be a good resource. Two such books are Hafner and Lyon’s Where Wizards Stay Up Late, and Jack Goldsmith and Tim Wu’s Who Controls the Internet: Illusions of a Borderless World. A reliable online resource is The Internet Society’s Histories of the Internet at http://www.isoc.org/internet/history.
5- See Wikipedia, “Domain Name System”, http://en.wikipedia.org/wiki/Domain_name_system for a more detailed account of the DNS.
6- See Wikipedia, “Generic Top-level Domain”, http://en.wikipedia.org/wiki/Generic_top-level_domain for a more detailed account of the TLD system.
7- For a definitive list, see http://data.iana.org/TLD/tlds-alpha-by-domain.txt. A more reader-friendly list is available at Wikipedia, “List of Internet Top-level Domain”, http://en.wikipedia.org/wiki/List_of_Internet_top-level_domains.
8- See “ISO 3166-1 alpha-2”, http://en.wikipedia.org/wiki/ISO_3166-1_alpha-2 for more details about ISO 3166-1 alpha-2.
9- The Berkman Center for Internet and Society, Accountability and Transparency at ICANN: An Independent Review: Appendix C: The Introduction of New gTLDs (2010), Harvard University, pp. 12-13, http://cyber.law.harvard.edu/pubrelease/icann/pdfs/AppendixC_gTLDs.pdf.
10- ICANN receives input from governments through the GAC. The GAC’s key role is to provide advice to ICANN on issues of public policy, and especially where there may be an interaction between ICANN’s activities or policies and national laws or international agreements. GAC issues communiqués after its meetings to report its activities and recommendations. For more information see https://gacweb.icann.org and http://www.icann.org/en/committees/gac/.
11- GAC, “GAC Comments on the Applicant Guidebook (April 15th, 2011 version)”, 26 May 2011, http://www.icann.org/en/topics/new-gtlds/gac-comments-new-gtlds-26may11-en.pdf.
12- ICANN, “New gTLD Draft Applicant Guidebook: Analysis of Public Comment”, 18 February 2009, http://www.icann.org/en/topics/new-gtlds/agv1-analysis-public-comments-18feb09-en.pdf.
13- Kevin Murphy, “UK-US corporate world slams ‘dot-brand’ domain plans”, The Register, 1 September 2011,

http://www.theregister.co.uk/2011/09/01/icann_generic_domain_plan_slammed_by_corporates/.
14- ICANN, “New gTLD Draft Applicant Guidebook”.
15- ICANN, “Public Comment: CRAI Report on gTLD Registries and Registrars”, 24 October 2008, http://www.icann.org/en/announcements/announcement-24oct08-en.htm; and Steve Salop and Joshua Wright, “Vertical Integration Between Registries and Registrars—The Economic Pros and Cons”, presentation made in Sydney, Australia on 22 June 2009, http://syd.icann.org/files/meetings/sydney2009/presentation-vertical-separation-22jun09-en.pdf.
16- European Commission, “Removal of vertical integration between registries and registrars for new and existing gTLDs”, http://www.icann.org/en/correspondence/eu-to-icann-17jun11-en.pdf.
17- Lawrence Strickling. “Cross-Ownership Issues for Registries and Registrars”, US Department of Commerce, 16 June 2011, http://www.icann.org/en/correspondence/strickling-to-dengate-thrush-16jun11-en.pdf.
18- GAC, “GAC Principles Regarding New gTLDs”, 28 March 2007, Clause 2.1, http://www.icann.org/en/topics/new-gtlds/gacprinciples-regarding-new-gtlds-28mar07-en.pdf.
19- ICANN, “New gTLD Program Explanatory Memorandum: Morality and Public Order Objection Considerations in New gTLDs”, 29 October 2008, http://www.icann.org/en/topics/new-gtlds/morality-public-order-draft-29oct08-en.pdf.
20- “GAC Communiqué—Nairobi”, 10 March 2010, https://gacweb.icann.org/download/attachments/1540146/GAC_37_Nairobi_Communique.pdf?version=1&modificationDate=1312226773000.
21- ICANN, “New gTLD Program Explanatory Memorandum: Limited Public Interest Objection (Morality and Public Order Objection)”, 12 November 2010, http://www.icann.org/en/topics/new-gtlds/explanatory-memo-morality-public-order-12nov10-en.pdf.
22- GAC, “GAC Comments on the Applicant Guidebook (15 April 2011 version)”, 26 May 2011, http://www.icann.org/en/topics/new-gtlds/gac-comments-new-gtlds-26may11-en.pdf.
23- ICANN, “GAC and Government Objections; Handling of Sensitive Strings; Early Warning”, 15 April 2011, http://www.icann.org/en/topics/new-gtlds/gac-objections-sensitive-strings-15apr11-en.pdf.
24- See Wikipedia, “Internationalized Domain Name”, http://en.wikipedia.org/wiki/Internationalized_domain_name for a more detailed account.
25- ICANN, “gTLD Applicant Guidebook”, 30 May 2011, http://www.icann.org/en/topics/new-gtlds/rfp-clean-30may11-en.pdf.
26- Panel at the Asia Pacific Regional Internet Governance Forum, 16-18 June 2011, http://2011.rigf.asia/transcript/04.pdf.
27- GNSO, “Outcomes Report of the GNSO Internationalized Domain Names Working Group”, 22 March 2007, http://gnso.icann.org/drafts/idn-wg-fr-22mar07.htm.
28- See Wikipedia, “IDN Homograph Attack”, http://en.wikipedia.org/wiki/IDN_homograph_attack for more details.

29- ICANN, “gTLD Applicant Guidebook”, 30 May 2011, pp. 2-8, http://www.icann.org/en/topics/new-gtlds/rfp-clean-30may11-en.pdf.
30- Wolfgang Kleinwächter, “De-Mystification of The Internet Root: Do We Need Governmental Oversight?”, in Reforming Internet Governance, William J. Drake, ed. (New York, UN ICT Task Force, 2005), pp. 209-225, http://www.wgig.org/docs/book/WGIG_book.pdf.
31- OECD, “Governments and business must tackle Internet address shortage together, says OECD”, May 2008, http://www.oecd.org/document/29/0,3343,en_2649_201185_40542045_1_1_1_1,00.html.
32- WSIS, Declaration of Principles – Building the Information Society: A global challenge in the new Millennium (12 December 2003), http://www.itu.int/wsis/docs/geneva/official/dop.html.
33- Yoshio, Utsumi, “Welcome Speech”, a statement to the First Meeting of the Working Group on Internet Governance, Geneva, Switzerland, November 2004, pp. 23-25, http://www.wgig.org/docs/Utsumi.pdf.
34- WGIG, Report of the Working Group on Internet Governance, June 2005, p. 4, http://www.wgig.org/WGIG-Report.html and http://www.itu.int/wsis/documents/doc_multi.asp?lang=en&id=1695%7C0.
35- WGIG, Background Report, June 2005, http://www.wgig.org/WGIG-Report.html and http://www.itu.int/wsis/documents/doc_multi.asp?lang=en&id=1661|1662|1663|1664.
36- See, for example, the letter by US Congressman Edward Markey as chairman of the Subcommittee on Telecommunications and the Internet in “Markey, Committee Members Comment on Possible Changes to Internet Watchdog Agency”, Office of Congressman Markey, 6 May 2008, http://markey.house.gov/index.php?option=content&task=view&id=3342&Itemid=125.
37- Milton Mueller, “XXX Puzzle Pieces Start to Come Together: And the Picture is Ugly”, CircleID, 17 August 2005, http://www.circleid.com/posts/xxx_puzzle_pieces_start_to_come_together_and_the_picture_is_ugly.
38- Directorate-General Energy and Transportation, “Galileo FAQ”, http://ec.europa.eu/dgs/energy_transport/galileo/faq/index_en.htm.
39- BCC, “Joint Strike Fighter Deal Agreed”, 12 December 2006, http://news.bbc.co.uk/2/hi/uk_news/politics/6173143.stm.
40- Lawrence Lessig, Code 2.0 (New York, Basic Books, 2007).
41- See Peng Hwa Ang, Ordering Chaos (footnote 1) for a fuller discussion.
42- OECD, “OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data”, http://www.oecd.org/document/18/0,2340,es_2649_34255_1815186_1_1_1_1,00.html.
43- John Perry Barlow, A Declaration of the Independence of Cyberspace, 8 February 1996, http://homes.eff.org/~barlow/Declaration-Final.html.
44- Ethel Quayle and Max Taylor, Child Pornography: An Internet Crime (New York, Brunner-Routledge, 2003).
45- Peng Hwa Ang, Ordering Chaos (see footnote 1).
46- Ibid.
47- Wikipedia, “Phishing”, http://en.wikipedia.org/wiki/Phishing.

48- Brad Templeton, “Reaction to the DEC Spam of 1978”, http://www.templetons.com/brad/spamreact.html.
49- Spamhaus, “The Definition of Spam”, http://www.spamhaus.org/definition.html.
50- See http://www.maawg.org/ and http://en.wikipedia.org/wiki/MAAWG for more details on the organization.
51- Julian Dibbell, “A Rape In Cyberspace”, The Village Voice, 23 December 1993, http://www.juliandibbell.com/texts/bungle_vv.html.
52- CNN, “Violators caught as Olympic video monitored on Internet”, 22 September 2000.
53- David Fickling and Stuart Millar, “How Diamond Joe’s libel case could change the future of the internet”, The Guardian, 11 December 2002, http://www.guardian.co.uk/technology/2002/dec/11/media.newmedia.
54- High Court of Australia, Dow Jones & Company Inc v Gutnick, [2002] HCA 56, 10 December 2002, http://www.austlii.edu.au/au/cases/cth/high_ct/2002/56.html.
55- Peng Hwa Ang, Ordering Chaos (see footnote 1).
56- See Wikipedia, “Cybersquatting”, http://en.wikipedia.org/wiki/Cybersquatting for more details.
57- See Wikipedia, “Reverse Domain Hijacking”, http://en.wikipedia.org/wiki/Reverse_domain_hijacking for more details.
58- WIPO, “Cybersquatting Hits Record Level, WIPO Center Rolls out New Services”, 31 March 2011, http://www.wipo.int/pressroom/en/articles/2011/article_0010.html.
59- Peng Hwa Ang, Ordering Chaos (see footnote 1).
60- Axel Metzger and Rita Matulionyte, “Opinion of European Academics On Anti-Counterfeiting Trade Agreement”, February 2011, http://www.iri.uni-hannover.de/tl_files/pdf/ACTA_opinion_11021 1_DH2.pdf.
61- European Parliament, “Resolution of 10 March 2010 on the transparency and state of play of the ACTA negotiations”, http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P7-TA-2010-0058+0+DOC+XML+V0//EN.
62- See Wikipedia, “Anti-counterfeiting Trade Agreement”, http://en.wikipedia.org/wiki/Anti-Counterfeiting_Trade_Agreement formore detail.
63- Intellectual Property Watch, “Still A Long Way To Go For Anti-Counterfeiting Trade Agreement”, 8 September 2011, http://www.ip-watch.org/weblog/2011/09/08/still-a-long-way-to-go-for-anti-counterfeiting-trade-agreement/.
64- Viktor Mayer-Schönberger, Delete: The Virtue of Forgetting in the Digital Age (Princeton, Princeton University Press, 2009).
65- Department of Information Technology, “Common Services Centers”, http://www.mit.gov.in/content/common-services-centers, last updated on 10 October 2011.
66- R. Kluver, “The Architecture of Control: A Chinese Strategy for e-Governance”, in “The Internet and Governance: The Global Context”, The Journal of Public Policy, vol. 25, No. 1 (2005), pp. 75-97.

UNITED NATIONS
ESCAP /APCICT

وزارت ارتباطات و فناوری اطلاعات
سازمان فناوری اطلاعات ایران

سازمان فناوری اطلاعات ایران
تهران -خیابان شریعتی - نرسیده به پل سید خندان - ورودی ۲۲
ساختمان مرکزی - کد پستی:۱۶۳۱۷۱۳۹۳۱
تلفنخانه: ۸۴۸۰۲۰۰۲
www.itc.ir

۹۷۸-۶۰۰-۷۶۳۱-۰۶-۵