

راهنمای
وبلاگ نویسان
برای
مقابله با سانسور



www.rsf.org

گزارشگران بدون مرز

راهنمای وبلاگ نویسان برای مقابله با سانسور

فهرست مطالب

- ۲..... - وبلاگ نویسان، منادیان جدید آزادی بیان/جولین پن.....
- ۵..... - وبلاگ چیست؟/ Pionblog.com
- ۹..... - انتخاب مناسب ترین ابزار/ Cyril Fievet و Mark – Olivier Peyer
- ۱۴..... - نحوه ایجاد و نگهداری یک وبلاگ/سیستم Civiblog لابراتوار شهروندان.....
- ۲۰..... - وبلاگ نویسان چه موارد اخلاقی را باید رعایت کنند؟/ دن گیل مور.....
- ۲۵..... - ورود وبلاگ شما به توسط موتورهای جستجو/اولیور آندریو.....
- ۳۲..... - چه چیزی باعث درخشش و شهرت یک وبلاگ می شود؟/مارک گلیسر.....
- تجربه های شخصی :
۳۵..... آلمان: ما از حقوق مدنی و بشر دفاع می کنیم/مارکوس بکداهل.....
- ۳۸..... بحرین: ما انحصار خیری دولت را شکسته ایم/چنعاد بحرینی.....
- ایالت متحده آمریکا: اکنون می توانم آن چه را که فکر می کنم، بنویسم
/جی روسن ۴۱.....
- هنگ کنگ: به عهد خود نسبت به کسانی که مردند، وفا کردم
/یان شام شاکلتون..... ۴۵.....
- ۴۸..... ایران: می توانیم آزادانه در وبلاگها بنویسیم/آرش سیگارچی.....
- نیپال: دنیا را از وقایع داخل مطلع می سازیم/
۵۱..... رادیو آزاد نیپال.....
- ۵۴..... -نحوه وبلاگ نویسی به صورت گمنام/اتان زوکرمن
- ۶۶..... -شیوه های فنی برای دور زدن سانسور/نارت ویلنیو.....
- ۸۶..... -اطمینان از ایمنی کامل پست الکترونیکی خود/لودویک پیرت.....
- ۸۹..... -جام قهرمانی سانسور اینترنت/جولین پن

وبلاگ نویسان

منادیان جدید آزادی بیان

نوشته ژولین پن*

وبلاگ ها در برخی افراد شور و هیجان برانگیخته و در برخی دیگر اضطراب و نگرانی را سبب شده است. برخی از مردم نسبت به وبلاگ ها بی اعتماد هستند. برخی دیگر وبلاگ ها را پیشگامان انقلاب جدید اطلاعاتی می دانند. یک چیز مسلم است: وبلاگ ها و کسانی که از آن استفاده می کنند در کشورهای مختلف از ایالات متحده گرفته تا چین و ایران، بنیان و اساس رسانه ها را به لرزه درآورده اند.

هنوز برای قضاوت در مورد وبلاگ ها، خیلی زود است. دهه های متمادی روزنامه ها را مطالعه کرده، تلویزیون تماشا کرده و رادیو گوش کرده ایم تا به واسطه آنها آموخته ایم که بین اخبار و پیشنهادات تمایز قائل شویم یا جمله های زرد مربوط به «علایق انسانی» را از روزنامه های جدی و برنامه های تفریحی تلویزیونی را از برنامه های مستند تشخیص دهیم.

برای تشخیص وبلاگ ها از یکدیگر چنین روش هایی وجود ندارد. این دفاتر خاطرات روزانه اینترنتی نسبت به رسانه های جمعی رایج متنوع تر بوده و تشخیص حوزه های خبری، حوزه های شخصی یا وبلاگ هایی که تحقیقات جدی انجام می دهند یا آنهایی که اسناد و شواهد غیر قابل استناد ارائه می دهند از میان آنها دشوار است. همان طور که جدا کردن گاه از گندم کاری دشوار است.

برخی وبلاگ نویسان به مرور زمان معیار های اخلاقی خاصی را تعیین می کنند تا به این وسیله اعتبار وبلاگ خود را افزایش داده و اطمینان مردم را جلب کنند. اما اینترنت همچنان پر از اطلاعات غیر قابل اطمینان بوده و همچنان مردم برای تبادل کلام ناپسند از آن بهره می برند. وبلاگ ها بدون توجه به سطح تحصیلات یا مهارت های فنی افراد به آنها اجازه می دهد تا اطلاعاتی را منتشر نمایند. به تعبیری دیگر وبلاگ های کسل کننده یا مبتذل نیز هم پا با وبلاگ های خوب و جالب پدیدار می شوند.

اما وبلاگ نویسی ابزاری محکم و قدرتمند در دست میلیون ها فرد عادی است که به آزادی بیان اهمیت می دهند.

مصرف کنندگان غیر فعال اطلاعات ، اکنون مشتریان پر و پا قرص این شیوه جدید روزنامه نگاری هستند - چیزی که پیشگام وبلاگ نویسی ایالت متحده دن گیللمور Dan Gillmor آنرا «روزنامه نگاری عامه مردم ... توسط مردم برای مردم» می خواند (برای کسب اطلاعات بیشتر به فصل مربوط به اصول اخلاقی وبلاگ نویسان مراجعه نماید).

در کشورهایی که رسانه های جمعی رایج تحت سانسور یا فشار قرار دارند ، وبلاگ نویسان تنها روزنامه نگاران واقعی به شمار می روند . تنها آنها می توانند اخبار مستقل را در اختیار مردم قرار دهند که با این کار خطرناک خشنودی دولت و گاه بازداشت را به جان می خرند. بسیاری از وبلاگ نویسان مورد آزار و اذیت قرار گرفته یا راهی زندان شده اند . یکی از افرادی که در نوشتن این کتاب راهنما به ما کمک کرد ، آرش سیگارچی بود که به علت درج چند مطلب انتقادی از رژیم حاکم در ایران به چهارده سال زندان محکوم شد . داستان او بیانگر احساس وظیفه و تعهد وبلاگ نویسان بوده و نشان می دهد که این کار تنها یک سرگرمی نیست . آنها خود را چشم و گوش هزاران فرد دیگر می دانند که از اینترنت استفاده می کنند .

وبلاگ نویسانی که انتشار اطلاعات توسط آن ها ممکن است خطرات امنیتی برای آنها به همراه داشته باشد باید گمنام باقی بمانند . پلیس حوزه های مجازی با دقت به دنبال افراد مشکل ساز بوده و اکنون راه پیگیری و پیدا کردن آنها را به خوبی می دانند . این کتاب راهنما روشهایی را به شما می آموزد که بتوانید بدون درج نام خود مطالبی را در این حوزه منتشر کنید (چگونه می توان بصورت گمنام وبلاگ نویسی کرد نوشته Ethan Zuckerman) . البته داشتن مهارت های فنی برای حفظ گمنامی در اینترنت بهتر است اما اجرای چند قانون ساده نیز می تواند موثر باشد . البته این آموزه ها و توصیه ها برای کسانی چون تروریست ها ، قاچاقچیان یا کودکان آزاران نیست زیرا آنها از اینترنت برای انجام جنایات خود استفاده می کنند . این کتاب راهنما تنها برای وبلاگ نویسانی است که به خاطر بیانات خود جهت حفظ آزادی بیان با مخالفت هایی مواجه هستند .

به هر حال ، خطر اصلی که وبلاگ نویسان فعال در رژیم های ستمگر را ، تهدید می کند ، مشکل امنیتی نیست . خطر اصلی شناساندن وبلاگ و یافتن گروه های مخاطب است . وبلاگی که مخاطب نداشته باشد از قدرت حاکم نیز باکی ندارد اما به چه دردی می خورد ؟ این کتاب راهنما برخی پیشنهادهای فنی را ارائه می دهد تا وبلاگ ها با اطمینان بیشتری از سوی موتورهای جستجو انتخاب شوند (مقاله نوشته شده توسط Olivier Andrieu) و برخی نکات روزنامه نگاری را یادآور می شود (چه چیزی باعث درخشش و موفقیت یک وبلاگ می شود ، نوشته Mark Glaser) .

برخی از وبلاگ نویسان با مشکل فیلتر گذاری مواجه می شوند . برخی رژیم های ستمگر اکنون ابزار فنی لازم برای سانسور اینترنت را در اختیار دارند . در کوبا یا ویتنام ، قادر نخواهید بود به سایت هایی که از دولت انتقاد نموده یا از فساد آن سخن گفته یا از نقض حقوق بشر می گویند ، دست پیدا کنید . متون درج شده در این حوزه ها از نظر دولت غیر قانونی و خرابکارانه بوده و بلافاصله توسط فیلترها مسدود می شوند . اما همه وبلاگ نویسان باید دسترسی آزاد به همه سایت ها ، حوزه های وبلاگ نویسی داشته باشند در غیر این صورت اصل وبلاگ آنها بی اثر خواهد بود .

بخش دوم این کتاب راهنما ، در مورد روش هایی برای رهایی از سانسور و فیلتر گذاری است (**انتخاب دور زننده ها نوشته Nart Villeneuve**) . با کمی خرد و درایت ، پشتکار و به خصوص انتخاب ابزار درست ، هر وبلاگ نویسی می تواند از دام سانسور رهایی یابد .

این کتاب راهنما برخی نکات فنی را در مورد نحوه راه اندازی یک وبلاگ خوب ارائه می دهد . اما داشتن و حفظ یک وبلاگ موفق کار بسیار دشواری است . برای سر برآوردن در میان جمع ، باید اصیل بوده و اخبار و عقایدی را منتشر نمایید که از سوی رسانه های جمعی رایج نادیده گرفته شده اند . در برخی کشورها ، تنها نگرانی وبلاگ نویسان این است که بتوانند از زندان رهایی یابند . در برخی دیگر ، چالش اصلی کسب اعتبار و تبدیل شدن به منبع قابل استناد اطلاعاتی است . همه وبلاگ نویسان با مشکلات یکسان رو به رو نیستند اما به طور کلی در خط مقدم مبارزه برای دستیابی به آزادی بیان قرار دارند .

** Julien Pain رئیس بخش آزادی اینترنت در سازمان گزارشگران بدون مرز است .*

وبلاگ چیست ؟

* Pointblog.com

وبلاگ به معنای وبسایت شخصی:

- بیشتر شامل اخبار است (متن نوشته شده) .
- همواره روزآمد می شود .
- به صورت دفتر روزانه است (که متون جدید در بالای صفحه قرار می گیرند) و همه متون نیز رده بندی شده و درج می شوند .
- با استفاده از ابزار خاص و محاوره ای ایجاد می شوند .
- عموماً توسط یک نفر طراحی و اداره می شود که گاه گمنام باقی می ماند .

متون درج شده در یک وبلاگ :

- معمولاً متن ساده (شامل برخی لینک های خارجی) ، گاه متن و عکس و جدیداً هم بیشتر صدا و فیلم است .
- کسانی که از وبلاگ ها بازدید می کنند قادرند پیشنهادات و نظرات خود را ارائه دهند .
- متون قبلی در وبلاگ ها بایگانی شده و امکان دسترسی به آن همیشگی است .

بنابراین می توان گفت که یک وبلاگ به صورت یک وبسایت شخصی است به استثنای این که :

- ایجاد و نگهداری آن بسیار ساده و آسان تر بوده و مرتب می توان اطلاعات آن را روزآمد کرد .
- سبک بسیار باز و منحصر به فردی داشته و دیدگاه ها با صراحت در آن ابراز می شوند .
- امکان بحث و گفت و گو با بازدید کنندگان و دیگر وبلاگ نویسان را ایجاد می کند .
- وبلاگ ها در سطح جهانی از ساختار استاندارد برخوردار بوده و از روش های یکسانی استفاده می کنند (ساختار دو یا سه ستونی ، پیشنهادات در زمینه موضوعات و RSS ها) .

زبان وبلاگ نویسی

بلاگ (وبلاگ)

خلاصه وبلاگ . پایگاه الکترونیکی که شامل متون کتبی ، لینک ها یا عکس هایی می شود که معمولا توسط یک نفر و برپایه ترجیحات فردی در آن جای می گیرند .

وبلاگ نویسی

داشتن یک وبلاگ یا درج مطالب در آن .

وبلاگ نویس

کسی که صاحب یک وبلاگ است .

وبلاگستان

همه وبلاگ ها یا جامعه وبلاگ ها

بلاگ رول Blogroll

لیست تمام لینک های خارجی یک وبلاگ به وبلاگ های دیگر که معمولا به صورت یک ستون در صفحه اصلی است . اغلب شامل برخی گروه های زیر مجموعه است که شامل دوستان وبلاگ نویس می شود .

Blogware

نرم افزار لازم برای ایجاد وبلاگ ها .

اسپم نظرات

همانند پیام های نامربوط / اسپمی که از طریق پست الکترونیک ارسال می شوند ، وبلاگ ها نیز از سوی مزاحمان تحت هجوم گسترده پیام های دروغین قرار می گیرند . این يك مشکل جدي بوده و وبلاگ نویسان و پایگاه های وبلاگ نویسی باید ابزار لازم برای حذف برخی از مشتریان یا پرهیز از ورود برخی آدرس ها به حوزه وبلاگ را در اختیار داشته باشند .

سندیکای محتوا (Content Syndication)

بیانگر این مطلب است که چگونه نویسنده یا مدیر یک وبلاگ، بخشی از مطالب خود را برای انتقال و نشر در پایگاه های الکترونیکی دیگر آماده می سازد .

موبلاگ

اختصاری که به جای عبارت وبلاگ های سیار استفاده می شود . این عبارت به وبلاگ هایی اشاره می کند که می توان آنها را از دور و از هر جایی با استفاده از تلفن یا ابزار های دیجیتالی روزآمد نمود .

لینک پایدار / پرمالینک

پرمالینک اسم اختصار عبارت لینک پایدار است و نشانی اینترنتی هر بخشی که بر روی یک وبلاگ منتشر شده است. این کار شیوه ی مناسب و پایداری برای ارائه نشانی هر مطلب حتی بعد از بایگانی آن در وبلاگ اصلی است.

وبلاگ های تصویری / فوتوبلاگ

وبلاگ هایی که بیشتر شامل عکس هایی هستند که بطور مداوم به صورت زمانبندی شده روی وبلاگ قرار می گیرند.

PODCASTING

تلفیقی از دو کلمه ی iPod و Broadcasting است که به معنای قرار دادن مطالب شنیداری و دیداری روی وبلاگ و روش های آسان برای قرار دادن اطلاعات روی پایگاه های الکترونیکی آن، برای استفاده در پخش کننده های دیجیتالی است.

پست

یک مطلب که روی وبلاگ ارسال شده، می تواند یک پیام یا خبر ، عکس یا پیوندی مجزا باشد. این اجزا معمولاً بسیار کوتاه بوده و دارای پیوندهای خارجی است و بازدید کنندگان می توانند درباره آن نظرات خود را بیان کنند.

(Really Simple Syndication) RSS

روشي آسان براي قرار دادن اطلاعات بر پايگاه هاي الكترونيكي بوده و براي وبلاگ ها بسيار مناسب است چرا كه به مشتركين در مورد روزآمد شدن مطالب يك وبلاگ خير مي دهد . همچنين با ايجاد اين فرصت براي پايگاه هاي الكترونيكي ديگر (به شيوه ساده و يا خود كار) براي باز توليد بخش يا كل مضامين يك پايگاه سبب افزايش نشر اطلاعات مي شود . اين روش بخصوص در پايگاه هاي الكترونيكي به سرعت در حال توسعه است.

RSS AGGREGATOR

نرم افزار يا خدمات آنلايني كه به وبلاگ نويسان امكان مي دهد RSS هاي مورد نظر خود بخصوص در مورد آخرين مطالب منتشر شده وبلاگ هاي مورد علاقه شان را مطالعه كنند . اين نرم افزار reader يا feed reader ناميده مي شود.

RSS FEED

فایلی كه حاوي آخرين مطالب منتشر شده يك وبلاگ باشد . اين فايل با استفاده از نرم افزار RSS AGGREGATOR / reader خوانده شده و در مورد روزآمد شدن اطلاعات يك وبلاگ خير مي دهد.

Trackback / دنبالك

شيوه اي كه به واسطه آن پايگاه هاي الكترونيكي با يكديگر ارتباط برقرار نموده و در مورد درج مطالب مرتبط با مطالب قبلي در همين وبلاگ يا وبلاگ هاي ديگر به هم اطلاع مي دهند.

Web Diary / دفتر خاطرات وبی

به معنای وبلاگ است .

WIKI

نام اين پايگاه الكترونيكي از يك كلمه در زبان هاوايي " wikiwiki " (به معنای سريع) گرفته شده است . اين پايگاه الكترونيكي بسيار ساده و سريع بوده و هر بازديد كننده اي مي تواند اطلاعات آن را به روز نمايد . امروزه اين كلمه را براي اشاره به ابزاري كه از آنها جهت ايجاد يك wiki (موتورهاي wiki) استفاده مي شود نيز بكار مي برند. وبلاگ ها و wiki ها شباهت هايي دارند اما ماهيت اصلي آنها متفاوت است .

انتخاب مناسب ترین ابزار

Mark – Olivier Peyer* و Cyril Fievet

وبلاگ ها حضور خود را مدیون پیشرفت و پویایی ابزار نشر هستند که تا حد زیادی عمل روزآمد نمودن پایگاه های الکترونیک را تسهیل نموده اند .

ابزاری که برای وبلاگ به کار می رود باید امکان کاربری مناسبی برای مصرف کننده داشته باشد تا از طریق مرورگرهای الکترونیکی به آسانی قابل دسترسی بوده و متن آن به شکل پویا اداره شود همچنین مواردی چون بایگانی و جستجو را نیز کنترل کند .

یک وبلاگ دارای دو آدرس اینترنتی است که بعد از برپایی آن نیز هرگز تغییر نمی کنند که عبارتند از :

- آدرسی که برای دسترسی عمومی تدوین و اعلام می گردد.
- آدرس مدیریتی آن که دارای رمز ورود بوده و در اختیار فردی است که آن را ایجاد کرده است .

شما می توانید با پیوستن به انجمن های وبلاگ نویس یا استفاده از ابزار وبلاگ نویسی با Server خود یک وبلاگ جدید ایجاد کنید.

انجمن وبلاگ نویسان

(برای کسب اطلاعات بیشتر به فصل " نحوه ایجاد و اداره یک وبلاگ : سیستم Civiblog " مراجعه نمایید)

طی چند دقیقه می توان به آسانی وبلاگی جدید را در میان گروه های مختلف وبلاگ نویس به وجود آورد . باید یک نام کاربری و یک رمز عبور انتخاب کرد سپس شما می توانید با فشار چند کلید وبلاگی جدید به وجود آورده و اداره کنید . برخی گروه ها برای ارائه این خدمات هزینه ای را در نظر می گیرند و برخی دیگر رایگان این امکان را فراهم می سازند .

اگر می خواهید وبلاگی را به وجود آورید که تنها برای مشاهده باشد ، این روش بهترین است. هزینه آن بالا نبوده (و بالاترین حد آن چند یورو در ماه است) ، بسیار آسان و سریع بوده و شما می توانید

از ترافیکی که توسط اعضای این گروه ها به وجود آمده یا از حسن شهرت آن بهره جویید .

اما مشکل این گونه از وبلاگ ها عبارتند از محدودیت های صفحه بندی و ویژگی های پیچیده. همچنین تبلیغاتی که از سوی گروه بوده و البته احتمال بسته شدن این سرویس ها نیز در آینده وجود دارد.

استفاده از ابزار وبلاگ نویسی

آنچه در پی خواهد آمد، ابزارهایی هستند که بر روی سرویس دهنده ها نصب شده و حاوی برنامه هایی برای راه اندازی خودکار یک وب سایت و یک بانک اطلاعاتی برای درج مطالب و نگهداری آن ها هستند . بعد از نصب ، این نرم افزار با استفاده از مرورگرهای اینترنتی استاندارد عمل می کند و برای اداره یک وبلاگ توسط آن ها نیازی به تخصص های خاص همچون نحوه استفاده از HTML نیست اما نصب و تنظیم آن ممکن است گاه با ترفندهایی همراه باشد نظیر تنظیم دسترسی ها، ایجاد بانک اطلاعاتی و تنظیم و راه اندازی سیستم های ارسال فایل یا FTP.

این راه حل برای افرادی است که با وبلاگ آشنایی دارند و مزیت آن این است که در صورت استفاده از آن، سایت کاملا متعلق به شما بوده و می توانید به راحتی آن را تنظیم کنید و به شکل مورد نظر خود در بیاورید و یا در هر زمانی نیز بتوانید آن را تغییر دهید؛ اما نیازمند برخی مهارت های فنی بوده و بیشتر نیز در معرض نظرات اسپمی و ناخواسته قرار گرفته و باید متون آن را نیز خودتان نگهداری نمایید .

چگونه باید انتخاب کرد که به کدام انجمن وبلاگ نویسان ملحق شد ؟

تغییر گروه ها و پیوستن به انجمن های جدید وبلاگ نویسی کار آسانی نیست، بنابراین در مرحله انتخاب درست ضرورت دارد .

قبل از انتخاب گروه مورد نظر باید موارد زیر را در نظر بگیرید :

گروه های زیر مجموعه یک انجمن بزرگ وبلاگ نویسان

برخی انجمن های بزرگ اینترنتی ، مصرف کنندگان خود را بر اساس علایق یا سن گروه بندی می کنند . گروه های زیر مجموعه یک انجمن وبلاگ نویسی بزرگ را بررسی کنید که دریابید آیا گروهی همانند با شما وجود دارد یا خیر .

شکل ظاهری وبلاگ ها

اگر چه انتخاب همیشه محدود است اما انجمن های مختلف (یا پلتفرم های متنوع) دارای رنگ ها ، فونت ها و شکل ظاهری صفحات متفاوتی هستند. با سر زدن اتفاقی به چند وبلاگ از هر انجمن وبلاگ نویسی و نگاه کردن به شکل ظاهری آن ها می توانید ایده ای درباره وضعیت ظاهری که هر یک از انجمن های وبلاگ نویسی در اختیار شما می گذارند، کسب کنید. بسیاری از گروه هایی که رایگان هستند از وبلاگ های کوچکتر می خواهند که در همه صفحات خود تبلیغاتی را جای دهند . همچنین ، در مورد حق انتخاب آدرس مورد نظر برای وبلاگ خود نیز تحقیق کنید . آدرس ها می توانند به قرار زیر باشند : <http://www.thecommunity.com/myblog> ، <http://myblog.thecommunity.com> یا <http://www.thecommunity.com/mynumber>

ویژگی های آرایه شده

بررسی کنید که آیا در صورت عضویت در گروه مورد نظر می توانید طراحی وبلاگ خود را تغییر داده ، افراد دیگری را نیز به جمع اضافه کرده ، تصاویر یا صداهایی را روی آن قرار داده ، مطالب را از طریق تلفن روی آن گذاشته یا دسترسی را (به صورت کامل یا مقطعی) به کاربران ثبت شده محدود کنید . همچنین بررسی کنید که آیا مطالب درج شده در وبلاگ را می توانید به گروه های دیگر ارسال نموده یا این که برای کسب درآمد بتوانید تبلیغاتی را در وبلاگ خود قرار دهید .

هزینه های پیش بینی نشده

برخی گروه ها امکانات رایگان فراهم می آورند اما پس از مدتی عضویت در آنها و خصوصا با توجه به میزان اطلاعات ذخیره شده و پهنای باند مورد استفاده باید مبلغی را به عنوان حق عضویت بپردازید . قبل از عضویت در انجمن ها این موارد را کنترل و بررسی کنید .

پایگاه ها و سکوی های بین المللی

<http://www.blogger.com> – Blogger

رایگان

در 1999 راه اندازی شد و در 2003 توسط گوگل خریداری شد و امروزه با هشت میلیون وبلاگ یکی از بزرگترین سرویس دهندگان است. استفاده از آن ساده است ولی گزینه های چندانی در اختیار شما نمی گذارد.

<http://www.livejournal.com> – LiveJournal

رایگان یا حدود 2 دلار در ماه یکی از قدیمی‌ترین سکوها است که شش میلیون وبلاگ بر روی آن وجود دارند، مخصوص وبلاگهای جوانان.

<http://www.msnspace.com> – MSN Spaces

رایگان
سکوی Microsoft که در اواخر 2004 راه اندازی شد. قابلیت‌های بسیاری دارد که گاهی از وبلاگ هم بیشتر است از جمله به اشتراک گذاشتن تصاویر و پیوند به Messenger. برای ثبت وبلاگ در این سیستم باید بیش از 13 سال سن داشته باشید.

سکوه‌های فارسی¹

توجه کنید که امکان فیلتر شدن اطلاعات وبلاگ شما یا دست یافتن حکومت به شما در صورتی که از سکوه‌های فارسی استفاده کنید بسیار بیشتر است چرا که این سکوها بیشتر در ایران کار می‌کنند و الزاماً تابع قوانین کشور هستند. قبل از شروع یک وبلاگ در این سکوها، به شکل دقیق مفاد قرارداد آنها را مطالعه کنید. در حال حاضر کلیه سرویس‌دهنده‌های وبلاگ فارسی سیستم خود را به شکل رایگان در اختیار کاربران قرار می‌دهند ولی در عوض تبلیغات مورد نظر خودشان را در وبلاگ شما به نمایش می‌گذارند.

<http://www.persianblog.com> – پرشین بلاگ

قدیمی‌ترین سیستم وبلاگ فارسی است و به همین دلیل پر استفاده کننده‌ترین. نسبت به دیگر سرویس دهندگان کیفیت پایین‌تری دارد ولی بسیاری از وبلاگ‌های فارسی زبان بر روی آن قرار دارند.

<http://www.blogfa.com> – بلاگفا

سیستم نسبتاً جدیدی است ولی به دلیل راحتی استفاده و قابلیت‌های بالاتر، بسیار مورد استقبال است. نسبت به دیگر سکوها سخت‌گیری کمتری نسبت به محتوای وبلاگ شما دارد و به گفته قراردادش به آزادی بیان احترام می‌گذارد ولی اجباراً تابع قوانین کشور است.

¹ در متن اصلی سکوه‌های فرانسوی معرفی شده بودند ولی به دلیل کاربرد بیشتر سکوه‌های فارسی برای ایرانیان، در ترجمه به جای آن سکوه‌های فارسی معرفی شده‌اند.

میهن بلاگ - <http://www.mihanblog.com>
از نظر کیفیت در سطح بسیار خوبی قرار دارد و در حال پیشرفت نیز هست ولی در حال حاضر بیشتر طرفداران حکومت از آن استفاده می‌کنند و سطح سانسور بالاتری دارد.

ابزارهای اصلی وبلاگ نویسی

DotClear - <http://www.dotclear.net>

MovableType - <http://www.movabletype.org>

Wordpress - <http://www.wordpress.org>

*هدف **Pointblog.com** این است که معنا و گستره این انقلاب مدرن اینترنتی را مشخص تر سازد . این پایگاه برای تازه کاران ، افراد خبره در این کار و حتی کسانی است که تنها از آن بازدید می کنند و دارای یک وبلاگ و چند بخش مستقل است. این پایگاه توسط **Pointblog SARL** اداره شده و توسط **Christophe Ginisty** و **Cyril Fievet** بنیانگذاری و مدیریت می شود.

نحوه ایجاد و نگهداری یک وبلاگ

سیستم Civiblog (www.civiblog.org)

روزآمد نمودن و نگهداری یک وبلاگ به مراتب آسان تر از یک پایگاه اینترنتی است. پایگاه های اصلی (یا سرویس دهنده های) وبلاگ روش های مختلفی برای درج اطلاعات دارند اما در اصول همه با هم مشابه اند. هدف از تحریر این بخش کمک به کسانی است که از Civiblog یا وبلاگ شهروندان استفاده می کنند، سیستمی که در همه جا توسط اعضای جامعه مدنی استفاده می شود، اما موارد ذکر شده در این بخش در مورد همه سرویس دهنده های مشابه نیز صادق است. Civiblog از پلتفرم نرم افزاری Blogware استفاده می کند که توسط شرکت Tucows به صورت آزاد و رایگان در اختیار همه قرار گرفته است.

ابتدا به بررسی برخی موارد می پردازیم که باعث مرسوم شدن و شهرت وبلاگ نویسی شده اند.

یکی از مهم ترین نکات فنی حوزه های وبلاگ نویسی درج آسان مطالب در آن است. یکی از نکات کلیدی «وبلاگستان» حضور RSS است. یک RSS در حقیقت یک عنصر XML است که به شکل خودکار توسط یک وبلاگ ساخته می شود و وبلاگ های دیگر می توانند به آن لینک بدهند. هنگامی که یک RSS feed را منتشر می کنید، این ابزار سر فصل های مطالب درج شده در وبلاگ را روی بخش خبری (برنامه های پست الکترونیکی مانند Outlook یا Thunderbird) قرار داده یا آن را مستقیماً وارد پایگاه الکترونیکی یا وبلاگ شخصی شما می کند. هنگامی که وبلاگ روزآمد می شود، RSS feed هم به همراه آن روزآمد شده و در نتیجه اطلاعات به صورت خودکار و با سرعت انتشار می یابند.

یکی دیگر از نکات فنی وبلاگ نویسی، دنباله است که نشان می دهد منشأ اصلی مطالب درج شده در وبلاگ از کجا بوده و از سوی اکثر پلتفرم ها مورد استفاده قرار می گیرد.

هنگامی که مطلبی مبتنی و یا برگرفته از یک وبلاگ دیگر باشد می توان امکان دنباله را به آن اضافه کرد تا به صورت خودکار تمام پایگاه هایی که این مطلب را باز تولید نموده یا در مورد آن پیشنهاداتی داشته اند، مشخص شوند. ممکن است این فرایند به نظر بسیار پیچیده باشد اما اجرای عملی آن بسیار ساده است و نتیجه رضایت بخشی هم دارد زیرا همواره دانستن این که دیگران نیز از

مطالب شما استفاده کرده و آن را در جایی عنوان کرده اند، لذت بخش است. همچنین این کار برای اشاعه هر چه گسترده تر مطالب و ایجاد آگاهی بیشتر نسبت به آنها و بسط و گسترش مباحث بین وبلاگ ها بسیار مفید است.

بنابراین هنگامی که قصد دارید وبلاگ خودتان را تهیه کنید کمی برای یادگیری این تکنولوژی وقت صرف کنید.

صفحه اصلی CIVIBLOG



RSS feed سمت راست قرار گرفته و هرگاه یکی از اعضای گروه مطلب جدیدی را درج کند، بطور خودکار روزآمد می گردد.

ثبت نام

قبل از برپایی يك وبلاگ ابتدا باید ثبت نام کنید. بسیاری از پایگاه های وبلاگ نویسی این کار را برای مشترکین آسان نموده اند. برای ثبت نام در civiblog تنها اطلاعات ساده و اولیه مورد نیاز هستند اما پایگاه باید اطمینان حاصل نماید وبلاگی که میزبانی آن را پذیرفته است واقعا متعلق به گروه های جامعه مدنی بوده و يك وبلاگ شخصی برای افراد

فامیل یا دوستان نیست. از زمان ثبت نام تا نمایان شدن On line وبلاگ تنها بیست و چهار ساعت وقت لازم است تا رمزهایی مورد نیاز برای دسترسی و ایجاد وبلاگ از طریق پست الکترونیک برای وبلاگ نویس ارسال شوند.

ورود به بخش مدیریت

وبلاگ دارای يك « صفحه » جلوی «صفحه ای که بازدید کنندگان آن را می بینند» و يك صفحه «پشت صفحه» است که شما با استفاده از نام کاربری و رمز ورودی که در زمان ثبت نام انتخاب می کنید می توانید برای روزآمد کردن و نظارت و راهبری وبلاگ خود به آن وارد شوید.

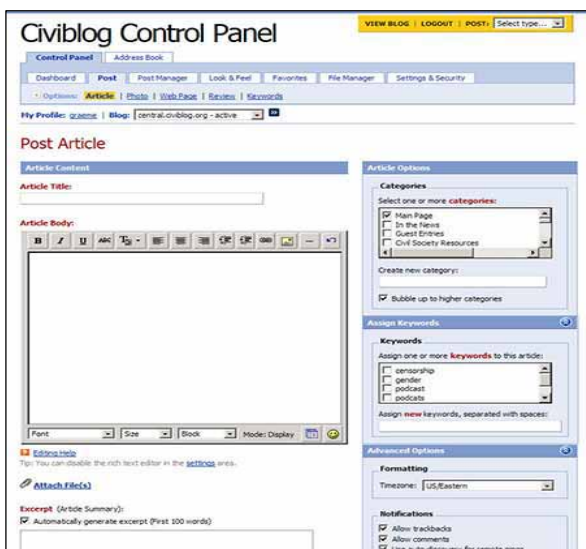
داشبورد

اکثر وبلاگ ها دارای یک صفحه داشبورد هستند یعنی صفحه ای پی برد چه چیزی در وبلاگش در حال رخ دادن است؛ از جمله آخرین ارسالها، آخرین نظرات و آخرین دنباله ها. شما می توانید از این صفحه به تمام تنظیمات وبلاگ دسترسی داشته باشید، از جمله ظاهر آن، پهنای باند مصرفی، ویرایش نوشته های قدیمی و تنظیم مجوزهای کاربران از جمله مجوز ارسال نظرات.



نحوه درج مطالب

بزرگترین تفاوت موجود بین وبلاگ ها و صفحات عادی سایت های دیگر این است که روزآمد نمودن وبلاگ ها بسیار آسان است. اکثر سکوها به شما این امکان را می دهند که در یک صفحه ساده مطالب خود را درج کنید بدون آنکه نگران صفحه بندی اش باشید. در پایگاه های جدیدی چون civiblo می توانید شکل حروف، اندازه و رنگ آن را تغییر داده و پیوندها و عکس هایی را وارد کنید.



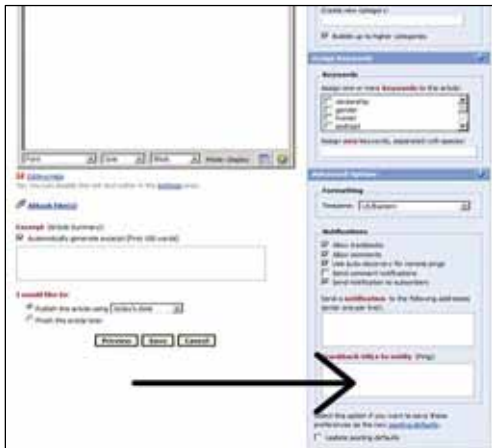
روش کار به شرح زیر است :

1. ورود به سیستم (Log in)
2. کلیک بر روی گزینه Post
3. در نظر گرفتن تیتری برای پیام مورد نظر و تایپ مطالب آن
4. صفحه بندی اطلاعات (Formatting) با استفاده از رابط های کاربری
5. گروه بندی مطلب (برای اینکه مطلب شما در کنار مطالب مشابه قرار گیرد) یا ایجاد یک گروه جدید

6. کلیک روی گزینه ذخیره (Save) که در پایین صفحه قرار گرفته است .
 به همین سادگی. با کسب کمی تجربه می توانید از ویژگی های دیگری چون دنباله، پینگ و کلمات کلیدی استفاده کنید .

دنباله یا Trackback

افزودن یک دنباله به مطلب نشر شده بسیار آسان است. شما باید نام URL مطلب مورد نظر را در جعبه سمت راست صفحه که با عنوان Trackback URLs to notify مشخص شده است وارد کنید. حالا وقتی که مطلب خود را ذخیره کنید به صورت خودکار این دنباله نیز ایجاد می شود.



سندیکای RSS (RSS Syndicate)

نشر RSS سایت های دیگر نیز بسیار آسان است:

1. وارد صفحه «پشت صحنه» وبلاگ شوید
2. روی گزینه Favourites کلیک کنید

3. روی گزینه RSS Headline Components کلیک کنید

4. مطابق دستورالعمل پیش رفته و URL (که به .xml، .rdf یا .py یا .php ختم می شوند RSS feed که می خواهید منتشر کنید را وارد نمایید .



۵. اسمی برای feed مورد نظر انتخاب کرده و گزینه Add feed را کلیک کنید
۶. حالا feed مورد نظر شما ساخته شده است و کافی است آن را وارد صفحه بندی وبلاگ خود کنید
۷. گزینه Look and Feel (شکل و ظاهر) را کلیک کنید
۸. گزینه Lay out (ساختار) را کلیک کنید
۹. روی گزینه RSS کلیک کنید : feed شما (همان اسمی است که در مرحله 5 به آن داده اید) را وارد ستونی کنید که می خواهید در آن نمایش داده شود
۱۰. روی گزینه ذخیره (Save) که پایین صفحه قرار گرفته کلیک کنید

در زیر نام برخی از پایگاه های الکترونیکی آمده است که ریزه کاری های وبلاگ نویسی را توضیح می دهند :

Civiblog Central Resources Blog:

<http://central.civiblog.org/blog/BloggingResources>

How to blog:

http://blogging.typepad.com/how_to_blog

The Blogosphere:

<http://blog.lib.umn.edu/blogosphere>

The Weblog Workshop:

<http://cyber.law.harvard.edu:8080/globalvoices/wiki/index.php/WeblogWorkshop>

Blogging 101:

<http://www.unc.edu/%7Ezucker/blogging101/index.htm>

وبلاگ نویسان چه موارد اخلاقی را باید رعایت کنند ؟

نوشته دن گیل مور*

همه وبلاگ نویسان به خبر نگاری علاقه ندارند. در اصل اکثر آنها خبرنگار نیستند. اما در صورت تمایل به چنین کاری باید اصول اخلاقی را رعایت کنند.

آیا این سخن بدان معناست که باید اصول اخلاقی خاصی را پذیرفته و امضا کنند؟ الزاما خیر.

کلمه حرفه ایی که برای اطلاق به آیین های اخلاقی در روزنامه نگاری از آن استفاده می کنند awash (مماس با لبه آب) است. برخی از این آیین های رفتاری از قانون اساسی ایالات متحده نیز طولانی ترند زیرا در آن ها تلاش شده است تا هر مورد احتمالی پیش بینی شده و در نظر گرفته شود. برخی دیگر نیز کوتاه و مختصر بوده و تنها اصول راهنمای ساده ای را ارائه می دهند. پایگاه الکترونیکی خبرنگاری در حوزه مجازی (سایبرژورنالیزم) با استفاده از جمعیت خبرنگاران حرفه ای که یک گروه آمریکایی است، آیین رفتاری را برای وبلاگ نویسان تهیه نموده است (<http://www.cyberjournalist.net/news/000215.php>). این حرکت کاری منسجم و ارزشمند است.

تدوین آیین نامه های رفتاری تنها برای رسیدن به یک هدف صورت می گیرد: القای اعتماد. اگر خواننده، بیننده و یا شنونده به گزارشی که در پیش رو دارد، اعتماد نداشته باشد، خواندن آن در وهله اول هیچ ارزشی نخواهد داشت. البته بدون شک استثنا هم وجود دارد که عبارت است از مطالعه موارد غیر اخلاقی برای درک کردن اصول صحیح و همچنین رسیدن به دانش درست. مصداق ضرب المثلی قدیمی ایرانی است که می گوید: ادب از که آموختی؟ از بی ادبان.

به نظر من همه اصول اخلاقی تنها در مورد یک مطلب بسیار ساده سخن می گویند: شرافت. هرچند که این کلمه، حوزه بسیار گسترده ای را در بر می گیرد اما به هر حال اگر شرافتمندانه برخورد نکنیم، نمی توانیم انتظار داشته باشیم که مردم نیز به ما اعتماد کنند.

در نظام روزنامه نگاری آمریکایی، اعتماد با مقوله ای همراه است که ما آن را بی طرفی می نامیم به این معنا که هدف از نوشتن یک مقاله ارائه دیدگاه های مختلف درباره یک موضوع و دادن این فرصت به خواننده است تا خود در این باره تصمیم بگیرد.

من عقیده دارم که بی طرفی، یک هدف ارزشمند و دست نیافتنی است زیرا همه ما در همه امور غرض ورزی های خاص خود را داریم .

در جهان خبرنگاری نوین که از ارائه سخنرانی به سوی مذاکره حرکت می کنیم، روزنامه نگاری اخلاقی کمتر مبتنی بر اصول و قواعد اخلاقی بوده و بیشتر بر پایه ارزش ها و اصولی استوار است که بنیان روزنامه نگاری شرافتمندانه را تشکیل می دهند.

روزنامه نگاری مطلوب بر ستون هایی استوار است که عبارتند از :
دقت ، صحت ، عدالت ، شفافیت و استقلال .

مرزهای جدا کننده این مفاهیم چندان واضح نیستند. همه آن ها مستعد تفاسیر گوناگونند و حاوی ظرایف بسیار. اما من فکر می کنم که همه آنها، برای روی آوردن به روزنامه نگاری شرافتمندانه موثر بوده و در روزنامه نگاری **On line** دستیابی به آنها امکان پذیر تر به نظر می رسد. اکنون هر کدام را بررسی می کنیم .

دقت

از هنگامی که گزارشگر بودم تا بعدها که ستونی در روزنامه در اختیار داشتم همواره هدفم این بود که هر چه بیشتر بیاموزم. به هر حال جمع آوری واقعیات و آراء، پایه و اساس خبرنگاری را تشکیل می دهند. هرگاه احساس می کردم 95 درصد از چیزی را که آموخته ام در متن نهایی جایی ندارد، لذت می بردم. بهترین گزارشگرانی را که می شناسم همواره تلاش می کنند تا با یک فرد دیگر هم صحبت کرده و اطلاعات را از دیدگاه یک منبع دیگر نیز کنترل کنند . (آخرین سوالی که همیشه در همه مصاحبه ها می پرسیدم این بود : در این رابطه با چه کس دیگری می توانم صحبت کنم ؟)

امروزه، «دقت» فراتر از پرسیدن سوال از کسانی است که نام و نشانی آنها در دفترچه راهنمای واقعی یا مجازی ما قرار دارد . بلکه به این معناست که در هر زمان ممکن از خوانندگان خود بخواهیم، داده های خود را ارائه کنند. یعنی همان کاری را که من در زمان نوشتن کتاب خودم درباره خبرنگاری گروه های مردمی در سال 2004 کردم (که بسیاری از نویسندگان نیز اکنون تلاش می کنند برای نوشتن کتاب های خود از این روش استفاده می کنند .) فشارهای رقابتی سبب می شوند که افراد کمتر به این موضوع توجه کنند اما من ایمان دارم که از این به بعد خبرنگاران بیشتر از این روش استفاده خواهند کرد .

صحت

همواره به واقعیات و مستندات تکیه کنید. سعی نکنید که تنها در مورد چیزهایی که می دانید صحبت کنید بلکه به چیزهایی که از آن اطلاعی ندارید هم اشاره کنید. (اگر به خواننده / شنونده / بیننده در مورد آنچه نمی دانید اطلاع دهید ، از او دعوت کرده اید تا خلا های اطلاعاتی شما را پر کند.) صحت به معنای تصحیح مسائلی است که درباره آن ها اشتباه کرده اید و همچنین اعلام این اشتباهات. انجام این کار به شیوه **On line** بسیار آسان تر است زیرا در این شرایط می توانیم زیان اشتباهات خود را در مورد خوانندگان جدید از بین برده یا حداقل کاهش دهیم .

عدالت

در عمل به همان اندازه که داشتن صراحت آسان به نظر می رسد، حفظ عدالت بسیار دشوار است. ما همیشه به چشم خودمان عادل به نظر می رسیم ولی در اینجا هم می توان چند قاعده جهانی را اعمال کرد. عدالت، دارای مفاهیم مختلفی بوده و مفهومی که در اینجا مد نظر است، شنیدن دیدگاه ها و نقطه نظرات دیگران و تلفیق آن در روزنامه نگاری است . البته این به معنای پذیرش و تقلید از دروغ ها یا تحریف هایی نیست که بعضی خبرنگاران حتی در صورت مشاهده قوت یک جنبه مساله به دیگر جنبه ها، به آن ها پناه می برند.

همچنین عدالت به معنای دادن فرصت به دیگران است که اگر تصور می کنند، شما دچار اشتباه شده اید نظر خود را بیان کنند. حتی اگر شما با نظر آنها موافق نباشید. مجددا تاکید می کنم که این کار به شیوه **On line** بسیار آسان تر از نشریات چاپی و برنامه های دیداری و شنیداری است .

در نهایت می توان گفت که عدالت حاصل یک وضعیت ذهنی است . همواره باید بدانیم که چه عواملی ما را پیش می برند و همیشه ظرفیت لازم برای شنیدن سخنان مخالفان خود را داشته باشیم . اولین قانون برقراری يك گفت و گو، شنیدن است. اطمینان دارم از کسانی که فکر می کنند من اشتباه می کنم بیشتر یاد می گیرم تا از کسانی که با من موافق هستند.

شفافیت

امروزه روشنگری به عنوان بخشی از روزنامه نگاری پذیرفته شده است . البته همیشه سخن گفتن آسان تر از عمل کردن است .

حتي به ظاهر هم نمي توان با اين عقیده مخالفت کرد که روزنامه نگاران باید برخي موارد خاص مانند اختلاف نظرهای منازعه آمیز مالي را آشکار سازند. اما حد و مرز این کار تا کجا باید باشد؟ آیا مي توان از همه خبرنگارانی که در حوزه های مختلف کار مي کنند انتظار داشت که سفره دل خود را براي همگان باز کنند؟ این کار تا چه حدي منطقي و درست است؟

تعصبات شخصي حتي تعصباتي که آگاهی نسبت به آنها وجود ندارد بر روي فرایند روزنامه نگاري نیز تاثیر مي گذارند. من يك آمریکایی هستم و با عقاید خاصی بزرگ شده ام که ممکن است مردمان سرزمین های دیگر (یا حتي برخي از افراد در ایالات متحده) صراحتاً آنها را نپذیرند. هر کسی باید از چیزهایی که بدون چون و چرا مي پذیرد آگاه بوده و در روند کار، هر از گاهی آنها را مورد بازبینی قرار دهد.

یکی دیگر از راه های شفاف عمل کردن، شیوه بیان داستان است. باید در حد امکان به منابع استناد کرده و مضامینی که در اختیار مردم قرار مي دهیم را با استناد به واقعیات و اطلاعات درست استحکام بخشیم. (شاید این کار بخشی از دقت و صراحت باشد اما به نظر مي رسد که در این بخش بهتر جاي مي گیرد.)

استقلال

روزنامه نگاري شرافتمندانه به معنی دنبال کردن موضوع در مسیری است که پیش مي رود. هنگامی که رسانه های جمعی ادغام شده و تبدیل به چند شرکت بزرگ مي شوند یا تحت کنترل دولت قرار مي گیرند، این موضوع اتفاق نمي افتد. مستقل بودن در روش **On line** بسیار آسان است. به راحتی مي توانید يك وبلاگ به وجود آورید. اما هیچ کس نیست که بپذیرد، شرکتهای تجاري و دولت روي وبلاگ نویسانی که تلاش مي کنند با استفاده از شیوه کاری جدید خود امرار معاش کنند، فشاری اعمال خواهند کرد.

جف جارویس، یکی از وبلاگ نویسان برجسته آمریکایی (buzzmachine.com) برخي ایده آل های دیگر را نیز اضافه مي کند. وبلاگ نویسان باید به اصول اخلاقی محاوره ارج بگذارند. او به چیزی اشاره مي کند که برای من از اهمیت زیادی برخوردار است و آن این است که: محاوره به درك متقابل مي انجامد.

در محاوره، اولین قانون گوش دادن است. اصول اخلاقی به گوش کردن بستگی دارد زیرا به این ترتیب است که ما مي آموزیم.

**Dan Gillmore*: بنیانگذار شرکت رسانه های مردمی است که هدف آن تقویت روزنامه نگاری مردمی و گسترش دسترسی آن است. اولین پایگاه الکترونیکی او *Bayosphere.com* واقع در بی اریا در سانفرانسیسکو است. او نویسنده کتاب «ما به عنوان رسانه ها» نیز هست: روزنامه نگاری مردمی توسط مردم و برای مردم (چاپ آوریل، 2004).



وبلاگ او :

<http://bayosphere.com/blog/dangillmore>

اضافه شدن وبلاگ شما به موتورهای جستجو

نوشته اولیوراندریو*

وبلاگ ها، خودشان وب سایت هستند بنابراین توسط موتورهای جستجویی چون google، yahoo و MSN شناخته می شوند. بنابراین طراحی پایگاه الکترونیکی از همان ابتدا باید به گونه ای باشد که به این معیارهای دسته بندی مکانیکی موتورها پاسخ دهد.

وبلاگ ها چند ویژگی درونی دارند که در صورت فهرست بندی درست و جای گرفتن در صفحات نتایج از سوی موتورهای جستجوگر انتخاب می شوند.

- با توجه به این که این وبلاگ ها معمولا در ابتدا به صورت مجموع خاطرات شخصی هستند، متون زیادی در آن درج می شود که احتمال انتخاب آنها را افزایش می دهد. موتورهای جستجوگر بطور معمول پایگاه هایی را که دارای طراحی گرافیکی یا تصاویر متحرک ساخته شده با نرم افزار Flash بوده و متن نوشته شده چندانی ندارند را انتخاب نمی کنند.
- هر «مطلب» که عموما یک صفحه را اشغال کند، از طریق پیوندی دائمی قابل دسترسی باشد و به بحث در مورد یک موضوع بپردازد، احتمال انتخاب شدن بیشتری نصبت به صفحاتی دارد که طولانی ترند و مباحث مختلفی در آن مطرح شده است (مانند بایگانی ها و یا صفحات اصلی وبلاگ ها).
- عنوان یک نشریه عموما در صفحه عناوین یا URL (نشانی) باز تولید می شود. بطور مثال در وبلاگ رادیو نپال آزاد به نشانی <http://freenepal.blogspot.com>، هر مطلب صفحه مخصوص به خود را دارد مانند <http://freenepal.blogspot.com/2005/04/state-vandalism-in-nepal.html>

عناوین این مطلب (state vandalism in Nepal)، (ویرانگری دولت در نپال) نه تنها در صفحه URL بلکه در صفحه مربوط به متن نیز آمده است. همانطور که در پایین نمایش داده می شود.



بنابراین عنوان مطلب بعد از نام وبلاگ قرار می‌گیرد در حالی که در صفحه اصلی وبلاگ به تنهایی نمایان می‌شود .
(<http://freenepal.blogspot.com>)

وجود عبارات توصیفی کلیدی در عناوین صفحات (بخش مربوط به عنوان <TITLE> در زبان HTML) و در URL های این اسناد معیار اصلی انتخاب توسط موتورهای جستجوگر هستند بنابراین نکته مهم این است که عنوان نشریات را طوری انتخاب کنیم که از سوی موتورهای جستجوگر برگزیده شوند .

- پیوندها هم مانند متون به صورت خودکار به وجود می‌آیند ، خصوصا پیوند به بایگانی ها (برای نمونه به سمت راست صفحه رادیو نپال آزاد که نمایش داده شده است مراجعه کنید) .

PREVIOUS POSTS
State Vandalism in Nepal
Peace Bond: Sign of Problems
Must-Read Stories: April 20
Municipal Election: For Covering Up the Death of Democracy
Articles of Interest: April 16
Attempts to Blur Borderlines
Articles of Interest: April 7
Press: Support King or Die
Vote for Radio Free Nepal!
Nepali Congress leader released from house arrest

این کار برای انتخاب شدن بسیار موثر است زیرا متن موجود در پیوند ها (که anchors نامیده می‌شود) عامل مهمی در ایجاد ارتباط با آن چیزی است که در جستجوگرها، جستجو شده است. بنابراین در این مورد، وجود کلماتی چون "state vandalism in Nepal" (ویرانگری دولت در نپال) در اولین پیوند یا عنوان "رادیو نپال آزاد" در همین پیوند میزان ارتباط صفحه با کلمات کلیدی مورد نظر را به شدت بالا می‌برد. همچنین صفحه ای که این پیوند ها را روی خود دارد (برای موتورهای جستجوگر صفحاتی که امکان فشار روی عبارت های آنها وجود دارد اهمیت بیشتری دارند) و صفحاتی که از سوی آنها نمایش داده می‌شوند، مرتبط تلقی می‌شوند .

چگونگی بالا بردن امکان انتخاب شدن يك وبلاگ

وبلاگ ها ویژگی های مفید درونی زیادی دارند که میزان و امکان انتخاب شدن آنها را بالا می‌برد . هنگامی که موتور جستجوگر به واسطه معرفی مکانیکی وبلاگ یا از سوی «عنکبوت» ها - که به دنبال پیوند ها هستند - شناسایی می‌شوند، شانس انتخاب شدن این گونه وبلاگ ها، به واسطه خواص ذاتی شان، بیشتر از وب سایت‌های استاندارد است. اما برای افزایش قابلیت رویت باید کمی جلوتر هم برویم .

در اینجا نکاتی چند برای رسیدن به این مرحله با استفاده از کلمات کلیدی مهم برگرفته از عنوان وبلاگ شما ذکر می‌شود .

۱. روی فناوری های تمرکز کنید که امکان انتخاب شما را افزایش می دهند

اگر پایگاه الکترونیک شما هنوز On line نشده، در مورد فناوری که برای این کار انتخاب می کنید (مانند Blogger ، Dotclear ، BlogSpirit ، Joub ، و بسیاری دیگر) دقت فراوان داشته باشید. فناوری ای را انتخاب کنید که بیشترین جزئیات مربوط به انتخاب شدن را در خود جای داده باشد :

- عنوان نشریه باید بطور کامل در صفحه عناوین (<TITLE> the tag) و همچنین در URL بطور کامل باز تولید شود (با توجه به این که این موضوع همیشه اتفاق نمی افتد زیرا در بعضی ابزارها به شکل خودکار بعد از چند کاراکتر، بقیه نام حذف می شود) .
 - ایجاد پیوندهای دائمی (پیوندهای صفحات حاوی یک متن خاص) باید امکان پذیر باشد .
 - فناوری انتخاب شده باید به شما امکان طراحی بالا و هر چه بیشتر شخصی کردن محیط وب سایتتان را بدهد. یعنی شما بتوانید از طراحی گرافیکی و صفحه بندی شخصی در آن استفاده کنید . مهارت فی شما در این زمینه باید تا حدی افزایش یابد که بتوانید از بیشترین عوامل موثر در برگزیده شدن پایگاه الکترونیکی خود از سوی موتورهای جستجوگر استفاده کنید .
- برای کنترل این موارد باید به پایگاه های الکترونیک که از این فناوری استفاده کرده اند، مراجعه کنید (همواره یک نمونه بارز خوب در آنجا وجود دارد) تا ببینید که چگونه نمایش داده می شوند. با این روش می توانید چیزهای زیادی را بیاموزید .

۲ . بهترین عنوان را برای مطلب خود انتخاب کنید

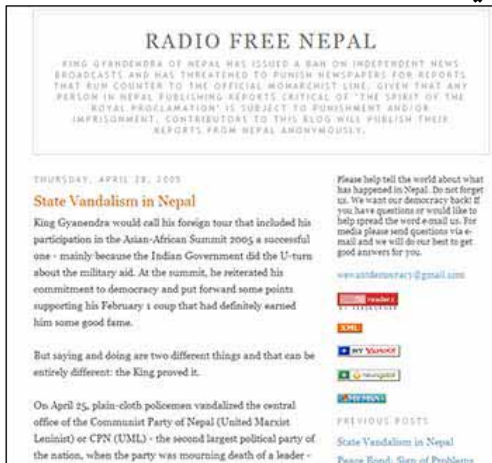
این نکته بسیار مهم است. عنوان مطلب شما در تک صفحاتی که نشان گر مطلب هستند، در URL ها و در متونی که پیوندهای ارتباطی به متن دارند، باز تولید می شوند. هر سه آنها مکان کلیدی جستجو برای موتورهای جستجوگر هستند. بنابراین بطور خلاصه می توان گفت که عنوان مطالب باید شامل مهم ترین واژه ها و عبارات باشد تا امکان انتخاب شدن وجود داشته باشد. از انتخاب عناوینی چون "چه خوش گفت!" "خوش آمدید!" "عالیه!" پرهیز کنید. عنوان باید در قالب کمتر از پنج کلمه بیانگر چیزی باشد که در متن مربوط به آن بیان شده است. به کلماتی فکر کنید که تمایل دارید موتورهای جستجو به واسطه آنها مطلب شما را انتخاب کنند و از آنها برای تعیین عنوان مطلب استفاده کنید. این کار ممکن است چندان آسان نباشد اما بسیار موثر است .

۳ . متن را آماده کنید

موتورهای جستجوگر عاشق متون هستند پس برایشان متن آماده کنید .

می توانید تا جایی که دلتان می خواهد عکس منتشر کنید اما فقط در صورتی که متنی نیز همراه آنها درج شود. سعی کنید که متن های شما حداقل 200 کلمه را در خود جای دهند زیرا این کار امکان برگزیده شدن آنها از سوی موتورهای جستجوگر را افزایش می دهد. همچنین از درج مضامین مختلف در یک مطلب اجتناب کنید زیرا موتورهای جستجوگر از این کار خوششان نمی آید. قانون طلایی در اینجا، یک مطلب، یک موضوع است.

۴. به اولین پاراگراف نوشته خود توجه کنید



جایگاه کلمات مهم در متن نیز از اهمیت بسیاری برخوردار است. در مورد پاراگراف اول دقت بسیار داشته باشید | بطور مثال اگر می خواهید با کلماتی چون "آزادی اسرا" که در متن شما به کار رفته است از سوی کاربران انتخاب شوید، سعی کنید که در 50 کلمه اول متن خود از این کلمات استفاده کنید. شرایط برای سایر کلمات کلیدی نیز به همین منوال است. صفحاتی که در ابتدایشان این کلمات را در خود جای داده اند در نتایج حاصل از موتورهای جستجوگر شرایط بهتری نسبت به صفحاتی داشته اند که در آنها کلمات کلیدی در

آخر ذکر شده اند (در حالی که همه موارد دیگر مشابه باشند). می توانید با برجسته کردن این کلمات، آنها را مشخص تر کنید. این علائم برای موتورهای جستجوگر بسیار مهم هستند.

۵. از درج مجدد متن پرهیز کنید

همه موتورهای جستجوگر مجهز به روش هایی برای متن های مشابه هستند و اگر 2 صفحه کاملاً مشابه باشند تنها یکی از آنها انتخاب شده و دیگری به ندرت در صفحه نتایج، نشان داده می شود. بطور مثال گوگل این پیغام را می دهد: (به منظور نشان دادن بهترین نتایج برخی از ورودی های را که مورد مشابه آنها وجود داشته، حذف کرده ایم. در صورت تمایل می توانید جستجو را تکرار کرده و موارد حذف شده را نیز ببینید.)

این شرایط برای وبلاگ ها بیشتر پیش می آید زیرا صفحات حاوی هر مطلب ممکن است بسیار شبیه به هم باشند. بطور مثال اگر مقدمه ای یکسان برای همه صفحات دارید، یا آن را در پایین صفحه یا تنها در صفحه اصلی ذکر کنید تا صفحات دیگر قابل تمایز از یکدیگر باشند.

۶. عنوان طولانی برای وبلاگ خود انتخاب نکنید

بهترین عنوان (محتویات قسمت <TITLE>) برای موتورهای جستجوگر بین 5 تا 10 کلمه است در صورتی که کلماتی چون حروف اضافه یا ربط در آن وجود نداشته باشند. عنوان صفحه وبلاگ عموماً از 2 قسمت تشکیل شده :

- عنوان کلی وبلاگ
- تکرار عنوان مطلب

بنابراین برای اینکه کلمات در صفحه عنوان اصلی از 10 تا بالاتر نروند باید برای عنوان کلی وبلاگ و برای عنوان مطلب هر کدام تنها 5 کلمه در نظر بگیرید. این کار چندان دشوار نیست اما رعایت اختصار در حالی که اطلاعات هم بطور کلی در آن نشان داده می شوند یکی از نکات کلیدی است که سبب می شود، موتورهای جستجوگر وبلاگ شما را انتخاب کنند.

اگر می توانید (همه فناوری ها این امکان را در اختیار شما قرار نمی دهند) ، عنوان مطلب را بالاتر از همه و عنوان کلی را بعد از آن قرار دهید ، حالت بر عکس آن چندان موثر نیست .

۷ . وبلاگ خود را عضو سندیکاها کنید

اکثر ابزارهای وبلاگ نویسی به شما امکان می دهند که يك "XML thread" یا "RSS feed" ایجاد نمایید که به این وسیله کاربران بتوانند با استفاده از نرم افزاری مناسب متن شما را برداشت نمایند. می توانید این تسهیلات را در وبلاگ خود به کاربران ارائه دهید (نصب آن تنها چند دقیقه طول می کشد). نه تنها تعداد بازدید کنندگان از وبلاگ شما افزایش می یابد که کلیه بازدید کنندگان Yahoo نیز که در جستجو به سایت شما برسند، لینک RSS شما را در کنار نتایج جستجو مشاهده خواهند کرد. در شکل زیر این موضوع نمایش داده شده است (View as XML).



بنابراین از این امکان استفاده کنید.

۸ . پیوندهای خود را همیشه روزآمد کنید

پیوندها بسیار مهم هستند زیرا به موتورهای جستجوگر اجازه می دهند تا صفحات سایت را به ترتیب شهرت آنها طبقه بندی کنند. (در Google این مورد PageRank نامیده می شود) با استفاده از روش های زیر می توانید تعداد پیوندهای وبلاگ خود را افزایش دهید :

- آن را وارد دایرکتوری ها کنید (برای کسب اطلاعات بیشتر به موارد زیر مراجعه کنید) .
- جستجو برای پایگاه های الکترونیکی که رقیب نبوده اما مطالبی را در مورد عنوانی همسو با وبلاگ شما ارائه می دهند موثر است.

تبادل پیوندها بین وبلاگ هایی که علائق و حوزه های مشابه دارند باید به سرعت انجام شود (این کار در انجمن های وبلاگ نویسی مکررا صورت گرفته و پذیرفته شده است و همین امر یکی دیگر از مزایای وبلاگ ها بشمار می رود) . وبلاگ ها برای این کار بسیار مناسبند زیرا حاشیه های آنها خالی بوده و به آسانی پیوند ها در آن درج می شوند .

دیده شده در وبلاگ در راهنمای موضوعات

دیده شدن در موتورهای جستجوگر عمومی (مانند Google ، MSN ، Yahoo و Exalead) و راهنماها (مانند Yahoo!Directory و Open Directory) بسیار مهم است اما دیده شدن در موضوعات خاصی نیز اهمیت بسیاری دارد چرا که :

- کاربران تخصصی را به وبلاگ شما راهنمایی می کند .
- تعداد پیوندها به وبلاگ شما افزایش می یابد که برای حسن شهرت شما مناسب است .
- باعث می شود شما توسط وبلاگ نویسان دیگری که بر روی همین موضوعات کار می کنند شناخته شوید و احتمال تبادل لینک بالا می رود .

در زیر برخی از ابزارهای جستجو (موتورهای جستجو و فهرست های راهنما) آمده است که وبلاگ ها را انتخاب می کنند :

English-language

Blogwise:	http://www.Blogwise.com/
Daypop:	http://www.daypop.com
Feedster:	http://www.feedster.com
Technorati:	http://www.technorati.com
Waypath:	http://www.waypath.com
Blogarama:	http://www.blogarama.com
Syndic8:	http://www.syndic8.com

French-language

Blogonautes	http://www.blogonautes.com
Blogolist	http://www.blogolist.com
Weblogues	http://www.weblogues.com
Blogarea	http://www.blogarea.net/Links/
Pointblog	http://www.pointblog.com
Les Pages Joueb	http://pages.joueb.com

فهرستی بزرگتر اینجا است:

http://search-engines.blogs.com/mon_weblogs/2005/05/les_search-engines_de_.html

همچنین به فهرست هر یک از ارایه دهندگان تکنولوژی هم نگاهی
بیاندازید، از جمله:

<http://www.canalblog.com/cf/browseBlogs.cfm>

<http://www.dotclear.net/users.html>

http://www.blogspirit.com/fr/communautes_blogspirit.html

نتیجه گیری

یک وبلاگ همه عناصر لازم برای انتخاب آسان از سوی موتورهای جستجوگر را در خود جای داده است. با نکاتی که در این بخش ذکر شد و رعایت آنها شما باید به نتایج خوبی رسیده و قابلیت رویت وبلاگ خود را افزایش دهید. بنابراین راه برای شما باز است و به یاد داشته باشید که " متن پادشاه است " .

*Olivier Andrieu** مشاور آزاد اینترنتی است که تخصص وی در کمک به وبلاگ
ها جهت انتخاب از سوی موتورهای جستجوگر است. پایگاه الکترونیکی
زیر نیز متعلق به اوست:

www.abondance.com

چه چیزی باعث درخشش و شهرت یک وبلاگ می شود؟

نوشته مارک گلیسر *

چه چیزی باعث می شود که از بین میلیاردها کلمه ای که توسط میلیون ها وبلاگ نویس در سراسر جهان انتشار می یابد، تنها یکی از وبلاگ ها مطرح و مشهور شود؟ چه چیزی نویسنده این وبلاگ را جزو قشر خاصی قرار داده و باعث می شود که خوانندگان هر روز به آن مراجعه کرده و نهایتاً افتخار و تمجید رسانه ای را برای او به همراه آورند؟

رابطه، پاسخ این سوال است. وبلاگ نویسان موفق کسانی هستند که با خوانندگان خود، چه ده نفر و چه ده هزار نفر، بواسطه ایجاد سرگرمی یا اطلاع رسانی رابطه برقرار کنند. بسیاری از مردم تمایل دارند که بین وبلاگ نویسان و دیگر نویسندگان (روزنامه نگاران ، رمان نویسان و کسانی که قلمی عامه پسند دارند) حد و مرزی قائل شوند اما هدف اصلی آنها مشترک است: یقه مردم را بچسبید تا از دستتان فرار نکنند.

برخی از وبلاگ نویسانی که در نوشتن این کتاب راهنما مشارکت داشته اند - مانند چنعد بجرینی از بحرین ، یان شام شاکلتون از هنگ کنگ و آرش سیگارچی از ایران - در کشورهای وبلاگ نویسی می کنند که دولت با دقت هر چه تمام تر بر کلمات آنها نظارت داشته و اینترنت را کنترل می کند. ولی از سویی دیگر جهانیان نیز آنها را نظاره می کنند و توسط آن ها از ماجراهایی باخبر می شوند که رسانه های جمعی این کشورها جرات بیان آن ها را ندارند. در چنین کشورهایی، آزادی بیان و آزادی مطبوعات در معرض خطر قرار داشته و صدای وبلاگ نویسان **On line** تنها ارتباط مهم با واقعیاتی است که در کوچه پس کوچه های شهر های آنها اتفاق می افتد. عکس هایی که آنها تهیه می کنند و داستان هایی که می گویند از اهمیت بسیاری برخوردار است.

اما چه چیزی باعث درخشش هر چه بیشتر این وبلاگ ها می شود؟ در زیر برخی ویژگی ها آمده است که باعث تفاوت و تمایز این وبلاگ ها از میلیون ها وبلاگ دیگر می شود .

صدایی منحصر به فرد و شخصی

بهترین وبلاگ نویسان با صدای خود سخن می گویند، به هویت منحصر به فرد خود افتخار می کنند و داستان هایی را بازگو می کنند که از نظر آنها واقعیت دارند. ایده وبلاگ برگرفته از مجلات **On line** است

یعنی يك مجله شخصي و بنابراین این نکته مهم را باید همواره به خاطر داشته باشیم که سبک نوشتن در وبلاگ مانند نوشتن مطالب دانشگاهی یا نوشتن برای رسانه های رسمی نیست. چنعداد بچريني نام مستعار يك وبلاگ نويس آسیايي است که در کشور عربي بچرين زندگي می‌کند و به همین دلیل نسبت به وقایع و رویدادهای این منطقه دیدگاهی متفاوت دارد. یان شام شاکلتون يك هنرمند اجرايي است که مدتی در اقصی نقاط دنیا زندگي کرده و تظاهراتی را علیه مسدود شدن سرويس دهنده وبلاگ TypePad توسط چین صورت داده است - در حالی که خود چند سال قبل به مقامات چین در فیلتر گذاري شبکه کمک کرده بود.

وبلاگ خود را همواره به روز نگه دارید

سکون و رکود یکی از اصلی ترین مشکلات همه وبلاگ ها است. با توجه به این که اکثر مردم براي وبلاگ نویسي پولي دریافت نمی کنند، پیدا کردن وقتی برای وبلاگ نویسي در زندگي هر روزه مدتي طول مي کشد. بسیاری از مردم وبلاگ نویسي را شروع می کنند، مدتی به آن ادامه می دهند و بعد دیگر هرگز وقتی براي به روز کردن اطلاعات آن پیدا نمی‌کنند. وبلاگ نویسان برای موفقیت باید مطالب خود را دائما به روز کنند و همچنین همیشه مشغول دنبال کردن موضوعات مورد علاقه خود و وقایع مرتبط باشند. البته این بدان معنا نیست که برای داشتن يك وبلاگ موفق باید 12 بار در روز مطالب را به روز کرد ولی مشخص است که يك رکورد چند هفته‌ای به راحتی می‌تواند باعث بی‌علاقگی و از دست رفتن مخاطبان شود.

با خوانندگان خود ارتباط برقرار نموده و آنها را توانمند سازید

یکی از ویژگی‌های متمایز کننده وبلاگ، امکان ایجاد ارتباط دوطرفه در آن است. راه های بسیاری براي درگیر نمودن خوانندگان وجود دارد که توسط آن ها می‌توانید افراد را وارد گفتگو کرده و از بازخوردشان (feedback) استفاده کنید. می‌توانید يك نظر سنجي On line بگذارید، آدرس پست الکترونیکی خود را در اختیار خوانندگان قرار دهید یا بحث مربوط به نظرات و پیشنهادات را فعال کنید. جف اویی بخاطر نظري که یکی از خوانندگان در مورد مطلبي نوشته بود از سوي دولت مالزي مورد تهدید قرار گرفت. اویی به جاي برداشتن همه پیشنهادات، تصمیم گرفت که پیشنهادات را مدیریت کند تا مطمئن باشد که خوانندگان تنها در مورد موضوع مورد بحث نظر می دهند و حاضر به پذیرش پیامدهای آن نیز هستند. او يك وبلاگ چيني زبان به نام The Ferryman را نیز براي ایجاد ارتباط بين وبلاگستان مالزیایی و چيني ایجاد کرده است.

در مقابل قدرت ، واقعیت را بگویید

در حالی که بسیاری از وبلاگ ها راوی نظرات نویسندگان هستند، برخی از آن ها به شیوه قدیمی به گزارش دهی مشغولند. برای انجام این کار یک روش تعریف شده وجود ندارد اما ارائه گزارش اصیل یا داشتن دیدگاهی خاص نسبت به یک مسئله باعث می شود که وبلاگ شما جنبه ای خاص پیدا کند. هنگامی که در نوامبر سال 2004 یکی از فعالان بحرینی زندانی شد، چنهاد بحرینی عکسها و صدای تظاهرات کنندگان در بحرین را در وبلاگ خود قرار داد و در موردی دیگر نیز وبلاگ نویس آرش سیگارچی به علت انتقاد از دولت تندروی ایران و همچنین اعتراض نسبت به دستگیری دیگر روزنامه نگاران، دستگیر و به 14 سال زندان محکوم شد. او بعدها با پرداخت جریمه آزاد شد اما پرونده اش همچنان باز است. (خاطر نشان می شود در زمان انتشار ترجمه این کتاب، این وبلاگ نویس که در دادگاه بدوی به 14 سال زندان محکوم شده بود، در دادگاه تجدید نظر حکومتی اش به سه سال کاهش یافت و در حال حاضر در حال گذراندن محکومیت در زندان است.) نکته اصلی این است که این وبلاگ نویسان و بسیاری دیگر همواره در مقابل قدرت ، واقعیت را گفته و این جسارت را داشته اند تا بعنوان یک نیروی جمعی در وبلاگستان در برابر مقاماتی که همواره واقعیات را پنهان کرده اند، بایستند .

Mark Glaser* ستون نویس «بررسی روزنامه نگاری On line» (www.ojr.org) است. نشریه ای است که توسط دانشکده ارتباطات آننبرگ وابسته به دانشگاه کالیفرنیا جنوبی منتشر می شود. او نویسنده ای آزاد است که در سانفرانسیسکو زندگی می کند. می توانید با این پست الکترونیکی با او تماس بگیرید: glaze@sprintmail.com



آلمان

ما از حقوق مدنی و بشردفاع می کنیم

نوشته مارکوس بکداهل*

در اواخر دهه 1990، زمانی که 20 ساله بودم، از نظر اجتماعی فعال شدم و برای رسیدن به جامعه اطلاعاتی آزاد و باز به لابی‌گری پرداختم. با کمک چند تن از دوستانم، سازمان غیر دولتی حقوق دیجیتال را با نام «شبکه رسانه‌های جدید» پایه‌گذاری کردم. به مدت پنج سال به ارتقای حقوق مدنی و انسانی در حوزه‌های دیجیتال پرداختیم. کنفرانس‌هایی را برگزار کردم و در مبارزات تبلیغاتی زیادی شرکت کردم و در شبکه‌های سازمان‌های غیر دولتی فعالیت داشتم. به طور مثال، ما کار هماهنگی «گروه هماهنگی جامعه مدنی آلمان» در WSIS را بر عهده داشتیم و انرژی بسیاری را صرف آماده شدن برای شرکت در کنفرانس جهانی جامعه اطلاعاتی کردیم.

در طول پنج سال اول فعالیت سیاسی از لیست‌های پست الکترونیک استفاده می‌کردم. من پنج هزار مقاله خبری و اعلامیه‌های مربوط به سیاست‌های شبکه‌ای را برای آنها ارسال کردم. اما این لیست تنها به تعداد محدود و مشخصی از کاربران ارسال می‌شد. از سوی دیگر، وبلاگ‌ها باز و شفاف بوده و فرصت‌های بیشتری را برای تبادل دانش و به اشتراک گذاشتن گزارش‌ها در اختیار کاربران قرار می‌دهند.

اولین وبلاگ من در سال 2002 همزمان با مرحله اول WSIS شروع به کار کرد. من در حالی به جلسه مقدماتی سازمان ملل متحد در ژنو آمدم که مجموعه وسایلم شامل یک کیسه خواب و یک نوتبوک بود. برای انتشار سریع گزارش‌هایم به زیرساختی احتیاج داشتم که بتوانم بدون نیاز به HTML مطالب را به سرعت در اینترنت قرار دهم. پیش از آن نشر اخبار با استفاده از HTML وقت زیادی را از من می‌گرفت. من در وبلاگی به نام «با کوله پشتی به سوی سیاست جهانی»، درباره تاثیر فعالیت‌های سیاسی خود در سطح سازمان ملل متحد نوشتم. این اولین وبلاگ من بود.

جدیدترین وبلاگ خودم را در بهار سال 2004 با نام netzpolitik.org راه اندازی کردم. قبل از شروع کارم با Wordpress که یک نرم افزار آزاد است و جامعه‌ای بزرگ پشت خود دارد، بسیاری نرم افزارهای دیگر را نیز آزمایش کردم. وبلاگ‌ها امکان ایجاد، ویرایش و نشر سریع متن را با کیفیت مناسب در اختیار من قرار می‌دهند. چیزی که برای من بیشتر از همه اهمیت دارد، رابط پیوندی است که به من اجازه می‌دهد بر کار اصلی خود یعنی نوشتن متن تمرکز کرده و وقت خود را صرف صفحه بندی مطالب با HTML نکنم.

من نیاز به یک رابط کاربر آسان دارم که از طریق آن بتوانم اطلاعات را گردآوری کنم، مقالات را بنویسم و با فشار یک دکمه آن ها را منتشر کنم. همه این ها کار مرا آسان می‌کنند. همچنین وجود فن آوری Push-Pull هم مفید است. بسیاری از افرادی که وبلاگ مرا می‌خوانند از Feed Readerها برای خواندن مطالب استفاده می‌کنند. دیگران، با استفاده از جستجوگرها یا موتورهای جستجو، مقاله های مرا پیدا می‌کنند.

با توجه به این که من عضو چند گروه سیاسی هستم، تلاش می‌کنم که همه اطلاعات مهم را در netzpolitik.org ثبت کنم که شامل این موارد است: حقوق مدنی و حقوق بشر، دنیای آزاد نشر متون، دسترسی آزاد و رایگان به دانش، جامعه اطلاعاتی و برقراری توازن در حوزه حق چاپ. آزادی بیان و آزادی اظهار نظر، شدیداً تحت تأثیر حق چاپ و مدیریت حقوق دیجیتال (DRM) قرار دارند. اما تعداد بسیار کمی از مردم از اهمیت این موضوع آگاهی دارند بنابراین من تلاش می‌کنم تا آگاهی مردم را افزایش داده و به این ترتیب به شهروندان کمک کنم تا از حقوق خود دفاع کنند. حقوق مدنی مردم در سراسر دنیا در خطر است، از جمله در آلمان. سطوح بالاتر امنیت برای شهروندان به معنای افزایش دائمی نظارت بر آنان است ولی عامه مردم آگاهی کمی نسبت به این موضوع دارند که این مساله همچنین به معنی کاهش دائمی آزادی‌های آنان است.

نرم افزار آزاد و رایگان (مانند سیستم عامل Linux) نیروی بالقوه بیشتری برای بیان و تلفیق آزادی بیان، کثرت گرایی و پایداری در عصر دیجیتال دارند. مشخص است که همه رایانه های من با سیستم Linux کار می‌کنند. من در مورد توسعه نرم افزارهای آزاد و درباره ابعاد سیاسی آنها نیز مطالبی نوشته و توضیح می‌دهم که کاربران جدید چگونه می‌توانند از این نرم افزارها استفاده کنند. من با جدیت موضوع رشد دایره المعارف های Wikipedia On line و همچنین مجوزهای خلاقیت های عمومی (CC یا Creative Commons) را دنبال می‌کنم. نوشته های من تحت مجوز CC رایج شده و من تا وقتی که نقل قول مانند مرجع اصلی باشد، نسخه برداری و انتشار کار خود را برای اهداف غیرتجاری تشویق می‌کنم.

نکته مهم دیگر این است که اینترنت چگونه می‌تواند به شیوه ای فعال از سوی سازمان ها و شرکت های جامعه مدنی مورد استفاده قرار گیرد. من مدیر پروژه و مشاور ارتباطات سیاسی در اینترنت و مبارزات ترویجی اینترنتی و دموکراسی اینترنتی بودم که طبقه بندی ای جداگانه در وبلاگ ها به شمار می‌روند. کار من تحلیل ابزار آزاد و رایگان برای ایجاد همکاری و عملگرایی و تمرکز بر جنبه های مختلف نرم افزارهای اجتماعی بوده و این که چگونه می‌توان در وسعتی گسترده تر، به شکل جمعی و اجتماعی آگاهی ایجاد کرد.

در netzpolitik.org، من اطلاعات و دانش مربوط به کنفرانس های آتی و همچنین مطالب سخنرانی ها و جلسات جامعه اطلاعاتی را نیز جمع آوری می کنم. گزارش کنفرانس های خود را تهیه کرده و نظر خود را در مورد آنها بیان می کنم. علاوه بر اینها، بخشی روزانه به نام نگاهی بر اخبار وجود دارد که شامل پیوندهای بسیاری است که در آن من نظر خود در مورد قوانین جدید و فعالیت های سازمان های غیر دولتی در این حوزه را بیان می کنم. وبلاگ من تبدیل به یک مرکز اصلی در بین جامعه مدنی و شبکه های آلمانی زبان شده که مطالب گوناگونی را برای گروه های مختلف اجتماعی تامین می کند. همچنین من گاهی از دوستان وبلاگ نویس خود می خواهم تا در مورد بعضی از مطالب کلیدی چیزی بنویسند یا اخبار را سریعتر منتشر کنند. من از خبرخوان RSS خود برای جمع آوری و بررسی سریع اخبار استفاده می کنم. در طول 10 ماه اول، من با کمک دوستانم توانستم بیش از 800 مطلب منتشر کنم.

در کمال تعجب باید بگویم که روزانه 2500 نفر وبلاگ مرا می خوانند. من بازخورد های بسیار خوبی بخصوص از جوانان دریافت می کنم و آنها را تشویق می کنم تا وبلاگ های خود را آغاز کنند. خوشبختانه، آلمان دارای قوانینی برای دفاع از آزادی بیان است. هیچ کس مرا به خاطر انتقاد از دولت به زندان نخواهد فرستاد. من شهادت کسانی را که تحت رژیم های دیکتاتوری به سر می برند و با به روز رساندن وبلاگ خود، زندگی خود را به خطر می اندازند، تحسین می کنم.

The screenshot shows a blog post from PRESSthink, dated August 14, 2008. The title is "Things I Used to Teach That I No Longer Believe" by Jay Rosen. The main text discusses the author's experience at a journalism professors' annual convention in San Antonio, TX, where he presented an installation from David F. Mustich. The text reflects on the author's past beliefs about journalism education and the current state of the profession. Key points include the author's realization that many journalism professors still believe in a "mission" that is no longer relevant, and the author's hope that a new generation of journalists will emerge who are not bound by these outdated beliefs. The post also mentions a panel discussion with Carl Swanson Strapp and a student named Dianne E. Smith.



newthinking communication، مدیر اجرایی **Markus Bechedahl**، 28 ساله، این سازمان مسوول فن آوری ها و راهبردهای بازمین است. او همچنین بنیانگزار دوم و رئیس سازمان غیر دولتی حقوق دیجیتالی **Netzwerk Neue Medien** است. نام وبلاگ او عبارت است از: www.netzpolitik.org

بحرین

ما انحصار خبری دولت را شکسته ایم

نوشته چنعد بحرینی

من به دو دلیل عمده وبلاگ خود را آغاز کردم : (الف) برایم جالب بود که بدون محدودیت ، موعده مشخص یا محدودیت‌های رسمی بنویسم و (ب) تلاش برای مشارکت و به راه انداختن بحث درباره موضوعاتی که بسیار کم در سطح رسانه های مرسوم محلی به آنها پرداخته می شود .

این روزها، تنها ایستگاه رادیویی و تلویزیونی بحرین مستقیماً تحت کنترل دولت قرار دارد و در نتیجه هیچ گزارش یا بحثی حتی از موضوعاتی که ارتباط بسیار کمی با وضعیت سیاسی منطقه دارند نیز از آنها پخش نمی‌شود. تمام روزنامه های محلی در اختیار بخش خصوصی هستند. بنابراین آزادی نسبی بیشتری از رسانه های دیداری و شنیداری دارند. با این حال، در رسانه های چاپی نیز شرایط چندان بهتر نیست زیرا سردبیران جرات انتقاد صریح از برخی افراد خاص با نفوذ مانند اعضای دولت یا خانواده سلطنتی را ندارند (خصوصاً از پادشاه و عموی او به عنوان نخست وزیر).

اما اینترنت ابزاری برای افراد است تا بتوانند آزادانه عقاید خود را در سطح عمومی ابراز کرده بدون این که نگران نظارت و پیگرد دولتی باشند. اگر چه دولت بحرین تاریخچه ای طولانی در نظارت و مسدودکردن وبسایت‌های سیاسی دارند اما به نظر می رسد که شرایط در یک یا دو سال گذشته کمی بهتر شده است اگر چه اخیراً، مجدداً شرایط رو به وخامت گذاشته است. علاوه بر این، راحتی راه اندازی وبسایت‌ها و نوشتن به صورت ناشناس در آنها (مانند مورد من) شرایط را برای دولت جهت انجام هر گونه اقدامی علیه نویسندگان دشوارتر می‌کند.

به این دلایل من احساس می کنم که نیاز به مباحثه آزاد و صریح در همه مسایل (شامل مسائل سیاسی) در هر جا - خصوصاً هنگامی که کشور به سوی دموکراسی حرکت می کند - وجود دارد و اینترنت نیز یکی از بهترین روش ها و ابزارها برای ابراز عقاید و آرا است. دیدن محمود (www.mahmood.tv) که یکی از وبلاگ نویسان پیشگام در بحرین است، و بیش از یکسال است که بدون هیچ مشکلی با دولت به وبلاگنویسی مشغول است، مرا تشویق به شروع کار کرد.

یکی از اهداف مهم وبلاگ من بحث و تحلیل رویدادهای بحرین است. اما با توجه به کمبود اطلاعات دست اول تلاش کرده ام تا کاری شبیه به روزنامه نگاری انجام دهم .

به این معنا که تا جایی ممکن تلاش کرده ام تا خود در مراسم مختلف (خصوصاً راهپیمایی‌های اعتراضی) شرکت کرده و سپس در وبلاگ خودم در مورد آنها نوشته و عکس‌ها را در دسترس قرار دهم.

اکنون در بحرین چندین وبلاگ موجود است و تلاش همه آنها بسیار مثبت است. اکنون فضایی ایجاد شده که در آن می‌توان با صداقت در مورد طیف گسترده‌ای از موضوعات صحبت کرد. من از وبلاگ‌های بحرینی دیگر چیزهایی آموخته‌ام که هیچ‌گاه نمی‌توانستم این اطلاعات را از جایی دیگر کسب کنم. وبلاگستان بحرین فقط یک جمعیت **On line** نیست بلکه بسیاری از وبلاگ‌نویسان بحرینی ماهانه جلساتی برگزار می‌کنند تا به شکل رو در رو در مورد برخی از موضوعاتی که در وبلاگ‌ها مطرح می‌شوند با یکدیگر گفتگو کنند.

با این حال اکثر فعالیت‌های **On line** در بحرین در تالارهای گفتگوی **On line** صورت می‌گیرد که زمانی طولانی است فعالیت خود را آغاز کرده‌اند (مثلاً در bahrainonline.org). وبلاگ‌نویسی هنوز در بحرین پدیده‌ای رایج نیست اما وبسایت‌های ما هم اکنون نقش «پل‌های ارتباطی» را به خود می‌گیرند (همانطور که حسین درخشان توضیح داده: <http://hoder.vom/weblog/archives/013982.shtml>). با توجه به اینکه اکثر وبلاگ‌نویسان در بحرین به انگلیسی می‌نویسند، ما می‌توانیم با مردم جهان ارتباط دو سویه داشته باشیم تا از طرف آنها به عنوان یک منبع اطلاعاتی موثق برای درک شرایط واقعی بحرین پذیرفته شویم.

بنابراین، بطور مثال، هنگامی که در فوریه سال 2005 سه تن از گردانندگان سایت bahrainonline.org دستگیر شدند ما در وبلاگ‌هایمان در این مورد نوشتیم و در نتیجه این خبر در جهان سریعتر از بحرین منتشر شد. سازمان گزارشگران بدون مرز در همان روز بیانیه‌ای صادر کرد. فکر می‌کنم که توجه جهانی که به سمت این موضوع جلب شده بود نقش بسیار مهمی در تصمیم‌نهایی دولت برای رهایی این سه نفر پس از چند هفته داشت. بطور کلی می‌توان گفت که وبلاگ‌های ما انحصار خبری دولت در مخابره اخبار بحرین به جهان خارج را شکسته است.

بطور کلی وبلاگ‌نویسان بحرینی به خاطر مطالبی که می‌نویسند از سوی دولت با مشکلی مواجه نشده‌اند اما با آغاز سال جدید شرایط تغییر کرده است. همانطور که قبلاً گفته شد سه نفر از گردانندگان تالارهای گفتگوی **On line** در فوریه به علت درج مطالبی که بیانگر تنفر و انزجار آنها نسبت به دولت بود دستگیر شدند. یکی از این

گردانندگان علي عبدالممام، وبلاگ شخصی خود را نیز دارد. همچنين در ماه آوريل، دولت اعلام نمود که صاحبان همه سايتها بايد اطلاعات خود را در وزارت اطلاعات به ثبت برسانند و در غير اينصورت مورد پيگرد قانوني قرار خواهند گرفت. اين مطلب نشان مي دهد که دولت هنوز به خوبي اينترنت و وبلاگها را درك نکرده و نمي داند که در صورت احساس خطر از سوي نويسندگان On line چگونه بايد با شرايط برخورد کند.

**چنعدا بحريني که اصالتا متعلق به آسيای جنوب شرقي است اکنون در <http://chanad.weblogs.usdot> بچرين زندگي کرده و وبلاگ خود را در آدرس <http://chanad.weblogs.usdot> دارد. او ترجيح مي دهد که گمنام باقي بماند .*

ایالت متحده آمریکا

اکنون می توانم آن چه را که فکر می کنم، بنویسم

*نوشته جی روسن

هنگامی که تحقیقات خود را در مورد نحوه وبلاگ نویسی آغاز کردم پاسخ های متفاوتی شنیدم. اما بخشی که مشترک بود این بود: باید مقالات کوتاه بنویسی. برخی می گفتند که سبک کار چنین است. برخی دیگر نیز عقیده داشتند که تنها این شیوه تاثیر مثبت دارد و بدین ترین آنها عقیده داشتند که این چیزی است که افراد پر مشغله در حال جستجو در وبسایتها به دنبال آن هستند. همه به من می گفتند که افراد وقت کافی برای مطالعه تحلیل های طولانی و متفکرانه تو را ندارند.

این موضوع باعث تردید من شد. تصمیم نداشتم که مقالات طولانی 2000 کلمه ای بنویسم؛ اما هنگامی که تلاش کردم تا ایده های خودم را که هنوز از زبان دیگران بیان نشده بود در قالب مقالات بیان کنم، این اتفاق افتاد و و بعد از چند مطلب توجه تعدادی از افراد به وبلاگم جلب شد (البته هنگامی که بخواهم می توانم کوتاه بنویسم). دیگر برای من حد و مرزی وجود نداشت: آزاد بودم تا خود موثرترین شیوه را انتخاب کنم و دریابم که **PressThink** قرار است چگونه چیزی باشد.

این که «مردم وقت ندارند...» از نظر من حرفی بی معنا بود و دیگر به آن اطمینان نداشتم. چنین نصیحتی باعث می شد که خودم را محدود کنم و نتوانم آنچه فکر می کنم را بنویسم. اما هدف کلی از شروع **PressThink** دستیابی به آزادی بود: « وای! اکنون من جمله خود را دارم. اکنون می توانم آنچه را که فکر می کنم بنویسم ». علاقه اصلی من بیشتر در حوزه کاربرانی بود که فرصت لازم برای مطالعه عمیق را داشتند و تعداد آنها برای من به هیچ وجه مهم نبود.

رویکرد من چنین بود: این جمله من است، **PressThink**... اگر دوست ندارید بازگردید. به شیوه ای بسیار ظریف و انتزاعی، وبلاگ من بخشی از بازار رسانه های جمعی را تشکیل داده و در رقابت با سایت هایی است که درباره بازی های نمایشی، فوتبال و سریال تلویزیونی **Law and Order** می نویسند. البته این حرف چندان هم درست نیست. **PressThink** یک شهروند آزاد با فضای داوطلبانه است و لازم نیست مانند یک کنشگر بازاری عمل کند. این تجربه من در طول چندین سال وبلاگ نویسی است.

باید به خاطر داشته باشید که وب در مسایل متفاوت و گاه متضادی سودمند است. برای اطلاعات مهم و فوری، برای گشت زنی در یک حوزه، برای صحبت و ارتباط دو طرفه و همچنین وسیله‌ای برای دسترسی به اعماق، یک ابزار کمک‌کننده به حافظه، کتابخانه‌ای در دسترس و یک فیلتر. عدم استفاده از یک وبلاگ برای نوشتن تحلیلهای طولانی تنها به این علت که کاربران این ایده را نمی‌پسندند از نظر وب امکان‌ناپذیر است. از نظر رسانه‌ها هوشمندانه است. من هم فعال حوزه رسانه‌ای نیستم! عجیب این است که همیشه سعی می‌کنم مطالب کوتاه و شیک بنویسم اما آنها همواره تبدیل به مقالاتی طولانی می‌شوند. تعدادی از خوانندگان نسبت به این موضوع اعتراض داشته‌اند. یکی از متداول‌ترین چیزهایی که می‌گفتند این بود: «کلی کلمه برای یک موضوع اشتباه» و این موضوع بعد از مدتی برای من جالب هم شد.

هر وبلاگ خوبی پیش از آغاز باید یک سوال از وب بپرسد: آیا نیازی به حضور یک چیز اصیل... به من هست؟ اما قبل از این که جواب این سوال را بیابید باید مدتی وبلاگ نویسی کنید.

عنوان **PressThink** از عباراتی چون **group think** مشتق شده است اما گروه در آن عبارت از رسانه است. این عنوان همچنین خلاصه شده دکتترین **Press Thinking** است که نوعی فلسفه رسانه‌ای است و روزنامه‌نگاران با آن زندگی می‌کنند و حتی می‌توان گفت که در رسانه‌ها به یک مذهب تبدیل شده است. موضوعاتی هستند که توجه مرا به خود جلب می‌کنند. تفکر رسانه‌ای چیزی است که من به عنوان نویسنده و منتقد به آن مشغول هستم. حتی زمانی که در وبلاگ خود می‌نویسم نیز این کار را می‌کنم.

هدف از این کار ارجحیت دادن به تفکر مطبوعاتی در برابر رویدادهای گذرای است که در مطبوعات رخ می‌دهد. سپس آن را امتحان می‌کنیم یا از دیگران می‌خواهیم این کار را بکنند. این چیزی است که معنای حقیقی این عنوان است. این وبلاگ «درباره» تفکر مطبوعاتی است و همچنین اسبابی برای ایجاد تفکر مطبوعاتی بیشتر است. تصور می‌کنم که بسیاری از وبلاگ‌نویسان وقت زیادی را صرف تفکر و انتخاب درست عنوان وبلاگ خود نمی‌کنند. اما در مورد من، تا زمانی که عنوان را انتخاب نکرده بودم، آمادگی لازم برای شروع وبلاگ را در خود نمی‌دیدم.

من تلاش می‌کنم تا انتقاد مبتنی بر ایدئولوژی مطبوعات دیگر را به افراد و سازمان‌هایی بسپارم که مشتاق به انجام این کار بوده و مهارت بسیاری در آن دارند. **PressThink** یک وبسایت برای بازبینی رسانه‌ها نیست، هرچند که من در آن درباره ناظران رسانه‌ها نیز نوشته‌ام. **PressThink** شکارچی «گرایش»ها نیز نیست ولی در آن درباره کشف این گرایش‌ها نوشته‌ام. من از جورج بوش حمایت نمی‌کنم اما تفکر مطبوعاتی او را می‌نویسم. همانطور که در مقدمه وبلاگ خود نوشته‌ام «تلاش می‌کنم تا پیامدهای داشتن این گونه از مطبوعات که داریم را کشف کنم.»

روزی کسی درباره «شیوه ای» وبلاگ نویسی از من پرسید. من رسانه ها را مطالعه می کنم، در بلاگ رولینگ گشتی می زنم و به دنبال مطالب جالب می گردم. بعد لینکها را جمع می کنم و نوشتن را شروع می کنم. یا کسی برای من ایمیلی می فرستد که منجر به ارسال یک مطلب می شود. گاهی هم اتفاقاتی رخ می دهد که من حس می کنم خوانندگان وبلاگم می خواهند نظر مرا در باره آن بدانند بنابراین یک مطلب می فرستم. چیزی که من در اختیار دارم استفاده از سبک های متفاوت به جای استناد به شیوه های تغییر ناپذیر است، شیوه هایی که دائما در حال تغییر و تبدیل به روش هایی آسان برای ارسال مطالب به PressThink هستند.

در یک مقاله ساده در PressThink مانند " کناره گیری و مرگ تدریجی روزنامه "

http://journalism.nyu.edu/pubzone/weblogs/pressthink/2005/03/29/nwsp_dwn.html

پنج بخش باید پر شوند: تیترا، سوتیتر، متن، و پی نوشتها (یادداشت ها ، واکنش ها و پیوند ها) و پیشنهادها. هر کدام از اینها سبک نوشتاری متفاوتی را می طلبند. تیترا، می گوید که متن درباره چه چیزی است و باید توجه خوانندگان را جلب کند. سوتیتر بیانگر مطلب بوده و شمه ای از داستان متن را ارائه می دهد. متن همان متن اصلی است که عموما دارای 1500 تا 2500 کلمه و 20 تا 30 پیوند دارد که هر کدام به نوبه خود بیانگر بخشی از داستان هستند. بخش پی نوشت به ویرایش و پیگیری مباحث گسترده تر در وبلاگستان می پردازد که شامل واکنش ها نسبت به نوشته من است. پیشنهادات آغازگر گفتگوها هستند.

مقاله ای در PressThink موفق است که همه بخش های آن، در مقابل هم قرار داده شوند و خواننده بتواند ارتباط بین آنها را به درستی درک کند. تا زمانی که واکنش های بعدی ، بازخوردها و پیشنهادات به مقاله اضافه نشوند(که این کار ، گاه بیش از یک هفته طول می کشد)مطلب وارد PressThink نمی شود. این چرخه یک مطلب در وبلاگ است. هنگامی که کار مقاله ای می گیرد (که یکبار می گیرد و یکبار نمی گیرد)، مقالات تبدیل می شوند به انجمنی (فرومی) برای تبادل نظر درباره آن موضوع و انجمن دقیقا چیزی است که «فکر می کند». البته شکی نیست که من در آغاز کار تصوری درباره این شیوه و منطقی که این روش به مقاله تحمیل می کند، نداشتم اما با سعی و خطا به آن پی بردم. به همین دلیل است که می گویم برای یافتن بهترین شیوه وبلاگ نویسی باید مدتی با آن کار کنید.

قبل از این که **PressThink** را آغاز کنم باید ایده‌های خود در مورد روزنامه‌نگاری و روزنامه نگاران را از طریق خود نگهبانانی که مواظب مطالب ورودی به روزنامه بودند، بیان می‌کردم. اما حالا که مجله خودم را دارم نیازی به این کار نیست و نگهبانان مطبوعات به وبلاگ من مراجعه می‌کنند تا بفهمند که من به چه چیزی فکر می‌کنم. تفاوت بسیار بزرگ است. حالا آزادی اندیشه دارم.

J Rosen* در دانشگاه نیویورک آموزش خبرنگاری داده و از سال **1986** در این دانشکده فعالیت داشته است. او از سال **1999** تا **2005** رییس دانشکده بوده است. وی در شهر نیویورک زندگی می‌کند و نویسنده وبلاگی در مورد روزنامه نگاری و مشتقات آن است که **PressThink** نامیده می‌شود (www.pressthink.org). این وبلاگ اولین بار در سپتامبر **2003** معرفی شد:

<http://journalism.nyu.edu/pubzone/weblogs/pressthink>



هنگ کنگ

به عهد خود نسبت به درگذشتگان، وفا کردم

*نوشته یان شام شاکلتون

حالا ساعت 12:23 چهارم ژوئن و شانزدهمین سالگرد فاجعه قتل عام میدان تیانانمن در پکن است. هنگامی که در سال 1989 این اتفاق افتاد من در تونلی بیرون دفتر خبری زین هوا در هنگ کنگ نشسته بودم که در آن اعتصاب غذایی جریان داشت. ما از دانشجویان چینی حمایت می کردیم. ما برای آنها و برای خودمان دموکراسی میخواستیم. ما دیگر نمی خواستیم که مستعمره بریتانیا باشیم و همچنین علاقمند هم نبودیم که به زیر سلطه حزب کمونیست برویم. ما آزادی می خواستیم.

دو یا سه ساعت بعد، صدای اولین تیر را از رادیو شنیدم و به دنبال آن صدای سرود، جیخ و انعکاس هجوم تانک ها از پشت دیوار به گوش رسید. هنگامی که به یکدیگر نگاه کردیم، اشک بر صورت همگان جاری بود.

همه می دانستیم که چین در مقابل دموکراسی خواهان از تانک استفاده خواهد کرد اما تا آن لحظه نمی توانستیم این را باور کنیم. فکر می کنم در آن زمان بود که **Glutter** در ذهن من متولد شد یعنی زمانی که پایان کار نهضت دموکراتیک را در سال 1989 در حالی که در یک تونل با نورهای فلورسنت نشسته بودم از رادیو شنیدم. در آن زمان 15 سال داشتم.

مدت کوتاهی بعد از این واقعه با خود عهد بستم. عهده که کمتر زنان بی تجربه ای مانند من، در دنیا ممکن است جسارت لازم آن را داشته باشند تا با عزمی راسخ از آن صحبت کنند:

" هرگز فراموش نخواهم کرد. قسم می خورم که تا ابد به یاد داشته باشم. من بخاطر خودم و همه، زندگی بهتری خواهم داشت زیرا من زنده ماندم ولی شما دیگر زنده نیستید. هرگز اجازه نمی دهم که این واقعه تکرار شود. من همواره دانشجویان میدان تیانانمن را به جهانیان یادآور خواهم شد. قهرمانان من. برادران و خواهران بزرگ من. "

من با شتاب، ترس و در کمال بی تجربگی این عهد را با خود بستم. هرگز با خود فکر نکردم که چگونه می توان به این اهداف دست یافت و آیا امکان آن وجود دارد.

اما فکر می‌کنم حق با من بود، همه بزرگسالان از درون بلندگوها همین چیزها را فریاد می‌زدند.

تنها امشب به این نتیجه رسیده‌ام که همه این نوشته‌ها، عکس‌ها و کارهای هنری که به نام دموکراسی انجام داده‌ام، مقاومت‌های اعتراضی که در حوزه مجازی سازماندهی کرده‌ام، مصاحبه‌هایی که در آن‌ها شرکت کرده‌ام، و داستان‌هایی را که تحت عنوان آزادی بیان منتشر نموده‌ام نه تنها به خاطر اعتقاد پر حرارت من نسبت به آنها بوده بلکه راهی برای تسکین ضمیر ناخودآگاهم نیز هست. وبلاگنویسی باعث می‌شود که به عهد خود نسبت به کسانی که مردند، وفا کنم. علت این که این موضوع را برای شما می‌نویسم این است که بدانید چرا **Glutter** را ایجاد و مدیریت کردم. زیرا این کار به پیروی از هیچ قانون خاصی یا با نسخه برداری از فرد دیگری صورت نگرفته است. من نمی‌خواستم توجه دیگران را به خود جلب کنم و یا شهرتی به هم بزنم. شاید خلوت بودن وبلاگ را ترجیح می‌دهم و هنگامی که توجه به وبلاگ زیاد می‌شود، مدتی آن را راکد باقی می‌گذارم چرا که تنها آن هنگام است که می‌توانم آنچه را که می‌خواهم بنویسم و داستانی که باید گفته شود را بدون حضور فشارها، به شیوه‌ای که دوست دارم نقل کنم.

نصیحت من به کسانی که می‌خواهند وبلاگی را آغاز کنند این است: به هیچکس جز خودتان گوش ندهید. سعی نکنید با مراجعه به وبلاگ دیگران از آنها تقلید کنید. با فهرستی از «بایدها» پشت وبلاگ ننشینید تا سعی کنید به آن‌ها دست پیدا کنید. من قوانین بسیاری را شکسته‌ام چرا که از آن‌ها اطلاع نداشتم و همه چیز نیز به خوبی پیش رفته است.

تنها چیزی که برای ایجاد یک وبلاگ به آن نیاز دارید اراده آغاز آن است.

تنها چیزی که برای ادامه یک وبلاگ به آن نیاز دارید این است که سابقه‌ای از هرآنچه گفته‌اید را داشته باشید.

هر کدام از ما لحظه به روشنی رسیدن از نظر سیاسی را تجربه کرده‌ایم، محرکی که باعث می‌شود به گونه‌ای از بی‌عدالتی پی‌بریم که باید اصلاح شود. در غیر این صورت به یک فعال اجتماعی که ایده‌ای برای خلق کردن دارد تبدیل نشده بودید. اجازه دهید که این درک، راهنمای شما باشد. امیدوارم که شما بتوانید به گونه‌ای مطالب خود را به دیگران انتقال دهید که آنها را نیز تحت تاثیر قرار داده و الهام بخش آنان برای مبارزه‌ای برای تغییر باشید. این تنها چیزی است که امشب می‌توانم به شما بگویم.

حالا ساعت 2:33 دقیقه صبح است و من می توانم صدای شلیک گلوله ها را بشنوم. هر سال همین موقع این صداها به گوش من می رسند. من 15 ساله بودم. سنم برای چنین تجربه هایی بسیار کم بود. اما آنهایی که مردند نیز برای مرگ جوان بودند.

*** Yan Sham Shackleton** می خواهد که شما هم بدانید که او 6 هفته را صرف نوشتن 6 نسخه از این مقاله نموده و تلاش کرده تا تمام دانش خود در مورد وبلاگ نویسی را منتقل کند و در نهایت به این نتیجه رسیده است که زیبایی این ابزار به آن است که بیانگر هویت فرد باشد.

او در وبلاگ خود **Glutter.com** از سیاست و هنر حرف می زند. صراحت کلام و موضع گیری شفاف او نسبت به دموکراسی واقعی در هنگ کنگ به این معناست که وبلاگ



او در داخل همواره اسیر سانسور است.

ایران

می توانیم آزادانه در وبلاگ ها بنویسیم

*نوشته آرش سیگارچی

امروزه ما حتی بهتر از خود مارشال مک لوهان این را درک می‌کنیم که «جهان یک دهکده جهانی است». خطوط نامرئی اینترنت به این معنا هستند که اگر چیزی در آسیا، آمریکا یا جزیره ای دورافتاده در آفریقا اتفاق بیافتد همه ما از آن با خبر خواهیم شد.

برای سال های متمادی روزنامه نگاری با محدودیت هایی مواجه بوده است اما با استفاده از فناوری می توان این موانع را برداشت.

من در کشوری روزنامه‌نگار هستم که موانع و محدودیت‌ها مانع از انجام فعالیت ام می‌شوند. علاوه بر عوامل درون سازمانی که در اکثر سازمان‌های رسانه‌ای جهان وجود دارند، اجزای برون سازمانی مانند محدودیت‌های قانونی، نفوذ دولت و افراد، حمایت یک جانبه از منابع خبری، گروه‌های فشار و سرمایه‌داران نیز نسبت به کشورهای پیشرفته از نفوذ بیشتری برخوردارند. بنا براین من وظیفه دارم که درباره استقلال کشور خود و انعکاس آن در اخبار واقعی و تحلیل خودم از اخبار فکر کنم. یکی از روش هایی که برای شکستن این موانع انتخاب کردم، وبلاگ‌نویسی بود.

ما می‌توانیم آزادانه در وبلاگ‌ها بنویسیم. با توجه به این که وبلاگ ها وارد حوزه چاپ یا بیان اخبار در رسانه های دیداری و شنیداری نمی شوند، نوشتن در آنها باعث انتشار سریع اخبار و دیدگاه‌های مختلف می‌شود. وبلاگ ها را می‌توان آژانس‌های خبری کوچکی دانست که نویسندگان آن هم نقش خبرنگار را بر عهده دارند و هم نقش سردبیر را..

برخی عقیده دارند که وبلاگ‌ها باید کمتر بر روی اخبار تمرکز کنند. مردم تمایل دارند که فعالیت‌های روزانه خود را در آن ثبت کنند. این نویسندگان نو پا مخاطبان کمتری داشته و اغلب دوستان و فامیل وبلاگ آنها را می‌خوانند.

اما وبلاگ هایی که متعلق به روزنامه‌نگاران و هنرمندان یا شخصیت‌های سیاسی، اقتصادی، اجتماعی و ورزشی برجسته است، حتی اگر مطالب آن تنها مربوط به زندگی روزمره آنان باشد، به علت ارزش خبری و حسن شهرت آنها مورد توجه قرار می‌گیرد.

مردم مطالب زیادی را دارند که می‌توانند آنها را مکتوب نموده و مخاطبان خود را جلب کنند. من عقیده دارم که هر وبلاگی افراد علاقه‌مند به این حوزه را جلب می‌کند، بنابراین هیچ محدودیتی در وبلاگ‌نویسی جایز نیست.

من دو روش برای وبلاگ‌نویسی انتخاب کردم، به صورت غیر رسمی و به شیوه عامیانه، نظر خود را در مورد وقایع جاری بیان می‌کنم. در شیوه دوم اخبار، تحلیل، مصاحبه، گزارش یا مقاله می‌نویسم. این کار باعث می‌شود که هر دو گروه خوانندگان را جلب کنم یعنی کسانی که می‌خواهند بدانند هم اکنون مشغول چه کاری هستم و هم کسانی که انتظار دارند بعنوان یک خبرنگار، نویسنده و شاعر دیدگاه‌های خود را بیان کنم.



وبلاگ‌ها بعنوان ابزاری On line به نویسنده فرصت می‌دهند تا دیدگاه‌ها و انتقادهای صریح خوانندگان را دریافت کرده، و یا به آنها پاسخ دهد یا خود را اصلاح کند. وبلاگ‌نویس در این رابطه نزدیک با خوانندگان، این امکان را دارد که با ابراز دیدگاه‌ها یا نوشتن مطالبی که خواننده از آن لذت می‌برد، آنها را در جهت درست سوق دهد.

همانطور که قبلاً گفتم اگر می‌خواهید کتاب، شعر، داستان، روزنامه یا مجله‌ای در ایران چاپ کنید باید از مقامات مجوز بگیرید. بسیاری از نویسندگان و روزنامه‌نگاران به خاطر این قانون دچار مشکل شده‌اند.

اگر بخواهید داستان، شعر یا مقاله‌ای را در روزنامه یا مجله‌ای چاپ کنید، سانسور می‌شود. بنابراین بسیاری از نویسندگان ایرانی دیدگاه‌های خود را با هزینه کمتر و بدون تجربه کردن فشار سانسور در وبلاگ‌ها منتشر می‌کنند. به همین دلیل دولت ایران نیز همانند چین و دیگر نقاط جهان استفاده از اینترنت را محدود می‌کند.

روزنامه‌نگاری اینترنتی باعث پیشرفت آزادی بیان و گسترده‌تر شدن دیدگاه‌ها می‌شود. اگرچه از سوی دادگاه‌های ایرانی محکوم شده‌ام اما امید خود را از دست نداده و مطمئن هستم که در سال‌های آینده مقامات کشورم به نشر آزاد اطلاعات و آزادی بیان احترام خواهند گذاشت.

*آرش سیگارچی ، روزنامه نگار و وبلاگ نویس ، در سال 1978 یعنی دوران انقلاب و براندازی شاه به دنیا آمده و در سال 1993 یعنی در 15 سالگی کار روزنامه‌نگاری را آغاز کرده است. زمانی که در سال 1997 رئیس جمهور اصلاح طلب جناب آقای محمد خاتمی انتخاب شد او به مطبوعات اصلاح طلب پیوست. بعد از آن در آوریل سال 2000 که این رسانه ها توقیف شدند، او برای زندگی به شمال ایران رفت و در آنجا سردبیر یک روزنامه 12 صفحه‌ای به نام «گیلان امروز» شد.



او در سال 2001 در یک وبلاگ گروهی به نام «گیله مرد» کار خود را آغاز کرد. در سال 2002 آرش سیگارچی پایگاه الکترونیکی خود به نام «پنجره التهاب» را شروع کرد. (www.sigarchi.com)

در اوایل سال 2005 از سوی وزارت امنیت و اطلاعات به مدت 2 ماه بازداشت شد و سپس به 14 سال زندان محکوم گردید. او هم اکنون آزاد و منتظر دادگاه تجدید نظر است. (رجوع شود به توضیحات صفحه 34)

نیپال

دنیای خارج را از وقایع داخلی مطلع می‌سازیم

*رادیوی نیپال آزاد

در تاریخ اول فوریه 2005 پادشاه جیانندرا بر اریکه قدرت نشست و مردم از طریق یک سخنرانی تلویزیونی از آن مطلع شدند. هنگامی که سخنرانی به پایان رسید، می‌خواستیم واکنش‌های بین‌المللی این تغییر و تحول را بدانیم و بنابراین تلاش کردیم به اینترنت متصل شویم. رایانه پیغام داد که هیچ خط تلفنی به آن متصل نیست. فهمیدیم که خطوط تلفن قطع شده‌اند. شاه برای جلوگیری از درز هرگونه خبر از نارضایتی مردم به خارج، به ارتش دستور داده بود که نه تنها مراکز ارائه دهنده خدمات اینترنتی را ببندد بلکه خدمات مخابراتی را نیز قطع کند.

در طول این مدت مردم در مورد پیامدهای مختلف این حرکت صحبت کرده و حتی برخی این حرکت شاه را تحسین می‌کردند. در دفتر روزنامه‌ای که من در آن کار می‌کردم همه آینده‌ای تاریک را پیش رو می‌دیدند زیرا مطمئن بودند که کارکنان ارتش به درون اتاق‌های خبری تلویزیون نفوذ کرده و اخبار را سانسور خواهند کرد. آن هنگام بود که فکر کردم نوشتن وقایع روزانه و افکار مردم به شکل یادداشت‌های مجزا اقدامی مناسب است. این کار را با استفاده از رایانه انجام دادم.

در تاریخ 8 فوریه خدمات اولیه مخابراتی و اینترنتی مجدداً فعال شد. بسیاری از افراد با ارسال پست الکترونیک از من می‌خواستند که وقایع نیپال را برای آنها توضیح دهم. در آن زمان تصور کردم که یادداشت‌های روزانه من می‌توانند به بهترین نحو شرایط را تشریح کنند. برخی از دوستانم در ایالات متحده آمریکا به من پیشنهاد کردند که یادداشت‌های هر روز را با تنظیم تاریخ روی روز نوشته شدن یادداشت‌ها، به اینترنت بفرستم. از آنجایی که من در امور وبلاگ نویسی کمی مبتدی بودم، آن‌ها این کار را برای من کردند. تصمیم گرفتم گمنام باقی بمانم و از دیگر دوستانم هم بخواهم که بدون اسم واقعی در وبلاگ‌ها بنویسند تا به این ترتیب از امکان رویارویی با دولت و آزار و اذیت و زندان در امان باشیم.

سانسورهای شدید رسانه‌های جمعی در اولین روزها و تبادل آزاد اطلاعات در رادیو نیپال آزاد، باعث شهرت روز افزون این پایگاه شده و Blogger.com نیز مردم را دعوت به دیدن این سایت می‌کرد. دوستان من در ایالات متحده آمریکا نهایت تلاش خود را برای شهرت هر چه بیشتر این سایت کردند. طی چند هفته، سایت کاملاً مشهور شده بود.

علت ایجاد رادیو نپال آزاد و هدف اصلی انجام چنین کاری این بود که مردم سراسر دنیا از احساسات تک تک مردم در مورد حکمرانی شاه با خبر شوند. رسانه های جمعی که تحت سانسور شدید قرار داشتند، تنها باید مطالب طبع میل پادشاه را می نوشتند و در نتیجه هیچ یک توان انعکاس احساسات واقعی مردم را نداشتند. اگر چه رادیو نپال آزاد حاصل تلاشی یک نفره و نیز مشارکت گاه به گاه چند تن دیگر بود اما به خوبی توانست بدون سانسور و بدون ترس از آزار و اذیت دولت، احساسات مردم را بیان کند.

مطالب اولیه رادیو نپال آزاد بیشتر به صورت یادداشت های روزانه بوده و رویدادهای روز را تشریح می کردند. ورودی های جدیدتر با تفکر و تحلیل وقایع همراه شده اند. در شرایط سیاسی نپال که پادشاه بدون در نظر گرفتن انتخاب مردم به زور قدرت را بدست گرفته است، رادیو نپال آزاد از اهمیت بالایی برخوردار است زیرا به مرکز بیان افکار عمومی تبدیل شده است.

در حقیقت چیزی که در کشورم به دنبال آن هستم، دموکراسی است چرا که معتقدم این تنها راه شکوفایی کشور است و چیزی است که به شغل من به عنوان یک روزنامه نگار معنا می دهد. نوشتن در شرایط سانسور مثل نوشیدن قهوه بدون شکر است، بی مزه! ما به عنوان یک روزنامه نگار، از چیزهایی اطلاع داریم که برای نوشته شدن هرگز جایی در روزنامه ها پیدا نمی کنند. مثلاً یکی از اخباری که در رادیو نپال آزاد درج شد در مورد اکتساب دارایی های شخصی به شیوه ای ناشایست از سوی شاه بود. بسیاری از روزنامه نگاران از این موضوع خبر داشتند، از آن انتقاد می کردند و درباره اش شوخی می کردند ولی هیچ جایی نبود که درباره آن بنویسند.

یکی دیگر از اهدافی که رادیو نپال آزاد توانست به آن دست یابد، اطلاع رسانی در مورد شرایط داخلی نپال به سراسر دنیا بود. اگر رادیو نپال آزاد به وجود نمی آمد ممکن بود که هزاران هزار نفر از مردم دنیا نسبت به شرایط نپال بی اطلاع بمانند. فکر می کنم که این روش برای برانگیختن افکار مردم در سراسر جهان بسیار مناسب بوده است.

پیشرفت های الکترونیک کمک شایانی به جامعه ما کرده اند. من آزادانه و بدون ترس می نویسم زیرا مطمئن هستم که شیوه وبلاگ نویسی من - یعنی نوشتن مطالب و ارسال آنها از طریق پست الکترونیک به دوستانم در ایالات متحده برای نشر - بدون استفاده از شیوه های بسیار پیچیده قابل پیگیری نیست. هنگامی که دموکراسی به کشور بازگردد و مردم آزادی داشته باشند، من احساس غرور خواهم کرد زیرا خواهم دانست که در رسیدن به آن نقش داشته ام.

خیلی‌ها با ارسال پست الکترونیک درباره اعتبار نوشته‌هایم از من سوال کردند. به آنها گفتم که یک نام نمی‌تواند مقیاس خوبی برای سنجش اعتبار باشد. نمی‌خواهم که تا زمان طلوع دموکراسی در نپال نام خود را فاش کنم زیرا ممکن است شرایط رو به و خامت گذاشته و من بخاطر وبلاگ نویسی راهی زندان شوم. از زندان نمی‌ترسم اما می‌خواهم به کار خود در رادیو نپال آزاد ادامه دهم. باید اخبار این کشور را به گوش جهانیان برسانم. من به آنها گفتم که پس از پایان کار حکمرانی این پادشاه، نام خود را فاش خواهم کرد.

تا آن زمان از همه شما به خاطر حمایتان تشکر می‌کنم .

**وبلاگ نویس رادیو نپال آزاد ، نپال
wewantdemocracy@gmail.com*

رادیو نپال آزاد وبلاگی است که علیه قدرت مطلق پادشاه جیانندرا و علیه سانسور رسانه‌های جمعی مقاومت می‌کند. رادیو نپال آزاد برای بازگرداندن دموکراسی به کشورش فعالیت می‌کند و اطلاعات به روز درباره شرایط داخلی را در اختیار جهانیان قرار می‌دهد. نویسندگان این وبلاگ به علت خطرات احتمالی که از سوی حکومت آنها را تهدید می‌کند به شکل گمنام می‌نویسند.

نحوه وبلاگ نویسی به صورت گمنام

*نوشته اتان زوکرمن

این راهنمایی فنی و سریعی است برای وبلاگنویسی گمنام. رویکرد این نوشته بررسی وضعیت در کشوری است که در آن دولتی غیرشفاف ممکن است به تعقیب وبلاگنویسان بپردازد. این راهنما برای سایبرپانکها نوشته نشده بلکه برای حمایت از افرادی نوشته شده که در کشورهای در حال توسعه نگران امنیت خود هستند و تلاش می‌کنند با حفظ ایمنی و خلوت خود، در اینترنت فعالیت کنند.

همچنین راهنمای موسسه Electronic Frontier Foundation تحت عنوان «چگونه با ایمنی وبلاگ بنویسم» متن بسیار خوبی در این مورد است (<http://www.eff.org/Privacy/Anonymity/blog/anonymously.php>).

فهرست

معرفی سارا

گام اول - نام‌های مستعار

گام دوم - رایانه‌های عمومی

گام سوم - Proxy های گمنام

گام چهارم - این بار شخصی است

گام پنجم - Onion Routing از طریق Tor

گام ششم - MixMaster ، Invisiblog و GPG

گمنامی تا چه حد لازم است؟ در این بحث تا کجا باید پیش رفت؟

معرفی سارا

سارا به عنوان حسابدار در یک دفتر دولتی کار می‌کند. او متوجه شده که رییسش، یعنی معاون وزیر، پول هنگفتی از دولت اختلاس کرده است. او می‌خواهد جهانیان را درباره جرمی که واقع شده مطلع کند اما نگران از دست دادن شغلش است. اگر این موضوع را به وزیر گزارش دهد (البته اگر بتواند وقت ملاقاتی بگیرد !)، ممکن است خودش اخراج شود. او با یکی از خبرنگاران روزنامه محلی تماس می‌گیرد اما خبرنگار می‌گوید که بدون در دست داشتن اطلاعات و اسناد کافی برای اثبات این ادعا، امکان درج آن در روزنامه‌ها وجود ندارد.

بنابراین سارا تصمیم می‌گیرد که اطلاعات خود درباره وقایع داخلی وزارتخانه را از طریق یک وبلاگ در اختیار جهان قرار دهد. او برای محافظت خودش باید اطمینان داشته باشد که هیچکس نخواهد توانست از طریق مطالب منتشر شده توسط او، به هویتش پی ببرد. او باید به صورت گمنام وبلاگ‌نویسی کند.

وقتی سارا سعی می‌کند که به شکل گمنام وبلاگ بنویسد، دو شیوه وجود دارد که ممکن است منجر به لو رفتن او بشود. اول این که او هویت خود را از طریق مطالبی که منتشر می‌کند فاش نماید - بطور مثال اگر در یکی از مطالب بنویسد: «من دستیار مدیر ارشد بخش حسابداری معاون وزیر صنایع و معادن هستم» عملاً به همه گفته است که چگونه می‌توانند به سادگی او را پیدا کنند. در شیوه دوم ممکن است دیگران بتوانند با استفاده از اطلاعاتی که مرورگرهای وب و برنامه‌های ایمیل به هنگام کار ایجاد می‌کنند او را شناسایی و دستگیر کنند. هر رایانه‌ای که به اینترنت وصل می‌شود دارای یک نشانی است که آن را IP می‌نامند. هر IP شامل 4 عدد بین صفر تا 255 است که با نقطه از یکدیگر جدا شده اند؛ بطور مثال : 213.24.124.38 یک IP است. هنگامی که سارا از مرورگر اینترنت خود برای ارسال یک نظر در وبلاگ وزیر استفاده می‌کند، آدرس IP او به همراه مطلبش ثبت می‌شود.

با کمی تلاش، کارشناسان فنی رایانه‌ای وزیر می‌توانند این نشانی را دنبال کرده و به هویت سارا پی ببرند. اگر سارا از رایانه خانگی‌اش استفاده کند تا با خط تلفن به یک مرکز ارائه دهنده خدمات اینترنتی (ISP) متصل شود، به احتمال قوی این سرویس دهنده نشانی IP اختصاص شده به سارا، شماره تلفن و ساعت کار او را ثبت می‌کند. در برخی کشورها، وزیر ممکن است برای گرفتن این اطلاعات نیاز به دریافت یک مجوز رسمی داشته باشد ولی در بعضی کشورهای دیگر (خصوصاً کشورهایی که ISP‌هایش متعلق به دولت هستند) این اطلاعات به آسانی در اختیار دولت قرار خواهند گرفت و سارا به دردر خواهد افتاد.

شیوه‌های گوناگونی وجود دارد که سارا می‌تواند با استفاده از آنها هویت خود را مخفی کند. به عنوان یک قانون کلی، هرچقدر که خواهان ایمنی بالاتری باشد، باید تلاش بیشتری هم انجام دهد. سارا یا هر کس دیگری که می‌خواهد به صورت گمنام وبلاگ نویسی کند قبل از شروع کار باید تعیین کند که چقدر نگران امنیت خود است و در نتیجه مشخص کند که تا چه حد حاضر به تلاش برای حفظ گمنامی‌اش است. همانطور که خواهید دید برخی از راهکارهایی که به منظور پنهان کردن هویت On line به کار می‌روند به دانش و تلاش فنی زیادی نیاز دارند.

گام اول - نام‌های مستعار

ساده ترین روشی که سارا برای پنهان کردن هویت خود می تواند استفاده کند، به کارگیری یک سرویس ایمیل رایگان و یک سرویس وبلاگنویسی رایگان خارج از کشور است. (استفاده از سرویس‌های پولی ایده جالبی نیست چرا که با پیگیری نحوه پرداخت دولت می‌تواند به شماره کارت اعتباری سارا یا اطلاعات حساب PayPal او پی برد و از این طریق به سادگی هویت او را آشکار کند). سارا به آسانی می تواند هویت جدیدی برای خود انتخاب کند - یک نام مستعار - و برای وارد شدن به سرویس‌های مورد استفاده اش از این نام مستعار استفاده کند. حالا وقتی که وزیر وبلاگ او را ببیند، اسم A. N. Ymous را به عنوان نویسنده خواهد دید که از ایمیلی با آدرس anonymous.whistleblower@hotmail.com استفاده می‌کند.

برخی از ارائه دهندگان شناسه‌های رایگان ایمیل عبارتند از:

Hotmail

Yahoo

Hushmail - ایمیل رایگان مبتنی بر وب با حمایت خوب از رمزگذاری

برخی از ارائه دهندگان سرویس وبلاگ جهانی عبارتند از :

Blogsom - وبلاگ های رایگان مبتنی WordPress

Blogger

Seo Blog

اشکال این روش کجاست؟ اشکال اینجاست که وقتی سارا برای استفاده از خدمات پست الکترونیکی یا وبلاگنویسی وارد سایت سرویس دهنده می‌شود، نشانی IP او در آنجا ثبت می‌شود. اگر امکان پیگیری این نشانی IP وجود داشته باشد - اگر او از رایانه خود در خانه یا محل کار استفاده کند و اگر شرکت ارائه کننده خدمات پست الکترونیکی یا وبلاگ مجبور به ارائه این اطلاعات به دولت باشد - هویت سارا فاش خواهد شد. البته اجبار شرکت های خدماتی شبکه جهانی برای ارائه این اطلاعات بطور مثال hotmail ، جهت یافتن نشانی IP سارا بسیار دشوار است و جناب وزیر برای این کار باید احتمالاً از طریق سازمان مجری قانون ایالات متحده آمریکا مجوز کسب کند. اما به هر حال سارا علاقمند نیست در این مورد ریسک کند.²

² توجه داشته باشید که در ایران بر اساس قانون، کلیه ISPها مجبور هستند کلیه ارتباطات کاربران خود را ثبت کنند و در صورت نیاز آن را در اختیار دولت قرار دهند. پس این شیوه از کار در ایران نیز ایمن نیست.

گام دوم - رایانه های عمومی

اقدام دیگری که سارا می تواند برای پنهان کردن هویت خود استفاده کند، استفاده از رایانه هایی است که عموم مردم از آن استفاده می کنند. او می تواند بجای این که حساب های کاربری وبلاگ و ایمیل خود را از رایانه خانه یا محل کار تنظیم کند، به کافی نت ها، کتابخانه ها یا دانشگاه ها مراجعه کند. در این صورت وقتی جناب وزیر نشانی IP یک مقاله یا اظهار نظر را پیگیری کند، تنها به کافی نت خواهد رسید که روزانه تعداد زیادی از مردم از رایانه های آن استفاده می کنند.

البته این روش هم مشکلاتی دارد. اگر کافی نت یا مرکز رایانه کتابخانه یا دانشگاه نام و زمان افرادی که از کامپیوترها استفاده می کنند را ثبت کنند، هویت سارا آشکار خواهد شد. او نباید نیمه شب از این مراکز استفاده کند زیرا تعداد مراجعه کنندگان کم بوده و فرد مسوول کامپیوترها ممکن است چهره او را بخوبی به خاطر بیاورد. در عین حال او باید همواره کافی نت محل مراجعه خود را تغییر دهد چرا که اگر جناب وزیر متوجه شود که همه مطالب افشاگرانه از کافی نت Joe's Beer and Bits در فلان خیابان ارسال شده اند کافی است یک نفر را برای زیر نظر گرفتن مشتریان در آن حوالی بگذارد و بعد از یک هفته به هویت سارا پی برد.

گام سوم - Proxy های گمنام

سارا از این که باید برای درج هر مطلب به کافی نت Joe مراجعه کند خسته شده است. او با کمک کاردان کامپیوتری که همسایه اش است رایانه اش را برای استفاده از یک Proxy گمنام تنظیم می کند. حالا هر وقت که بخواهد می تواند به پست الکترونیک و وبلاگش دسترسی داشته باشد. از این به بعد هر وقت که از ایمیل یا وبلاگش استفاده کند یا در جایی نظری بنویسد، شماره IP پروکسی سروری باقی خواهد ماند که به آن متصل است و نه شماره IP واقعی خودش؛ به این ترتیب کار یافتن او برای جناب وزیر بسیار دشوار می شود. در ابتدا او باید فهرستی از پروکسی های On line بیابد، اینکار به سادگی با جستجو به دنبال عبارت Proxy Server در گوگل عملی است. سارا برای اینکار به سایت publicproxyservers.com مراجعه می کند و یکی از پروکسی هایی که با عبارت «گمنامی بالا» (High Anonymity) مشخص شده است را انتخاب می کند. برخی فهرست های پروکسی های قابل اطمینان برای استفاده عموم عبارتند از:

- Publicproxyservers.com - پروکسی های گمنام و غیر گمنام
- [Samair \(http://www.samair.ru/proxy/\)](http://www.samair.ru/proxy/) - تنها پروکسی های گمنام و همچنین شامل اطلاعاتی درباره پروکسی هایی که از SSL پشتیبانی می کنند.

• **Rosinstrument proxy database** (<http://tools.rosinstrument.com/proxy>) - بانک اطلاعاتی قابل جستجوی پروکسی‌ها

سارا سپس بخش **Prefrences** (تنظیمات) مرورگر خود را باز می‌کند. در بخش **General** یا **Network** یا **Security** می‌تواند قسمتی را پیدا کند که حاوی اطلاعات اتصال به اینترنت از طریق پروکسی است (در مرورگر روباه آتشین (firefox) این گزینه را می‌توانید در بخش **Prefrences** و بعد **General** و سپس **Connection Settings** پیدا کنید).

او **Manual proxy configuration** یا تنظیم دستی پروکسی را روشن می‌کند، **IP** آدرس و همچنین پورت پروکسی **HTTP** یا **SSL**ی که انتخاب کرده است را در آن وارد و تنظیمات را ذخیره می‌کند. مرورگرش را می‌بندد و دوباره باز می‌کند و به شکل ناشناس مشغول گشت‌زنی در اینترنت می‌شود.

سارا متوجه شده که سرعت کارش با اینترنت کمتر شده است. دلیل این امر این است که هر صفحه‌ای که او می‌خواهد ببیند از یک راه فرعی به دستش می‌رسد. او به جای اینکه مستقیماً به **hotmail.com** متصل شود، اول به پروکسی‌اش وصل می‌شود و بعد پروکسی او را به **hotmail.com** متصل می‌کند. همچنین وقتی که **hotmail.com** صفحه‌ای را برای او می‌فرستد این صفحه اول به پروکسی می‌رود و بعد از آنجا به دست او می‌رسد. در عین حال سارا متوجه شده است که گاهی برای وصل شدن به بعضی سایت‌ها مشکل دارد، بخصوص در دسترسی به سایت‌هایی که باید به آن‌ها لاگین کند. ولی لاقلاً از این مطمئن است که آدرس **IP** او در جایی ثبت نمی‌شود.

حالا یک تجربه بانک با پروکسی‌ها: به سایت **noreply.org** بروید، یک سایت مشهور ارسال مجدد ایمیل. این سایت موقع ورود **IP** شما و محلی که از آن به اینترنت متصل شده‌اید را می‌گوید: «سلام **wma.east.verizon.net** به شماره آی.پی. **151.203.182.212**، خوشحالم که شما را می‌بینم.»

حالا به سایت **anonymizer.com** بروید، سایتی که به شما اجازه می‌دهد به شکل گمنام در (بعضی از) صفحات اینترنت گشت بزنید. در جعبه متنی بالای سمت راست صفحه آدرس قبلی یعنی <http://www.noreply.org> را وارد کنید. جالب است که حالا سایت **noreply.org** فکر می‌کند که شما از **vortex.anonymizer.com** به اینترنت متصل هستید. (**anonymizer.com**) یک پروکسی سرور گمنام‌کننده و رایگان است برای مواقعی که می‌خواهید بدون تنظیمات خاصی در مرورگرتان، به شکل گمنام وارد اینترنت شوید ولی این سرویس برای ورود به سیستم‌های پیچیده‌تری همچون ایمیل و وبلاگ‌نویسی مناسب نیست).

در نهایت این را هم امتحان کنید که با روش تشریح شده در بالا به مرورگر خود بگویید تا از یک پروکسی سرور استفاده کند و سپس دوباره به سایت noreply.org سر بزنید و ببینید که این سایت فکر می‌کند شما از کجا آمده‌اید.

اما افسوس که پروکسی‌ها هم کامل نیستند. اگر سارا در کشوری زندگی کند که در آن اینترنت سانسور می‌شود، مردم برای عبور از سانسور از پروکسی‌ها استفاده خواهند کرد. در این حالت ممکن است دولت سرویس دهندگان اینترنت را مجبور کند که سایت‌های پروکسی را نیز مسدود کنند. حالا کاربران به سمت پروکسی‌های جدید جذب خواهند شد و دولت دوباره آن‌ها را خواهد بست و این حلقه ادامه پیدا خواهد کرد. این روند مطمئناً پول و وقت بسیاری را هدر می‌دهد.

سارا یک مشکل دیگر هم دارد. اگر او یکی از معدود افرادی باشد که از یک پروکسی استفاده می‌کنند و با این روش در جایی نظری بدهد یا وبلاگی بنویسد، این احتمال وجود دارد که دولت با پیگیری آدرس IP پروکسی را بیابد و پس از بررسی سوابق ثبت شده در ISP‌ها پیدا کند که چه افرادی در چه تاریخی به آن پروکسی متصل بوده‌اند. مشخص است که دولت نمی‌تواند ثابت کند که این فرد از طریق پروکسی فلان مطلب را نوشته است ولی می‌تواند نشان دهد که این مطلب توسط فلان پروکسی نوشته شده و این فرد یکی از معدود افرادی است که دقیقاً در همان لحظه از آن پروکسی استفاده کرده است. سارا برای غلبه بر این مشکل از پروکسی‌های مشهور استفاده می‌کند و دائماً نیز پروکسی مورد استفاده خود را تغییری دهد.

گام چهارم - این بار شخصی است

سارا نگران این مسئله است که پروکسی‌های مورد استفاده او نیز تحت کنترل دولت قرار گیرند. اگر جناب وزیر موفق شود که با استفاده از راه‌های قانونی یا پرداخت رشوه، مسوول خدمات پروکسی را وادار کند تا نشانی همه کاربران را کنترل کرده و ببیند که آیا کسی از داخل کشور از این پروکسی‌ها استفاده می‌کند و - در صورت مثبت بودن جواب - چه کسانی، چه اتفاقی خواهد افتاد؟ سارا برای حفاظت از خود متکی به مسوولان پروکسی‌ها است در حالی که حتی آنها را نمی‌شناسد؛ هرچند که در اکثر مواقع گرداننده پروکسی نیز هرگز متوجه نخواهد شد که او کیست چرا که پروکسی‌ها معمولاً تصادفی باز گذاشته می‌شوند.

سارا دوستانی در کانادا دارد. به نظر می رسد که این کشور در مقایسه با کشور سارا سانسور بسیار کمتری دارد پس این امکان وجود دارد که دوستش بتواند در حفظ هویت وی و نگهداری وبلاگ به او کمک کند. سارا تلفنی با دوستش تماس گرفته و از او می خواهد که یک **Circumventor** را روی رایانه اش ایجاد نماید. **Circumventor** یکی از برنامه هایی است که مردم می توانند از طریق آن پروکسی هایی روی کامپیوترهای خود اجرا کنند و به دیگران اجازه بدهند تا با استفاده از آن از فیلتر رد شوند.

دوست سارا که جیم نام دارد یک **Circumventor** را از وبسایت (<http://www.peacefire.org/circumventor/simple-circumventor-instructions.html>) متعلق به مجموعه **Peacefire.org** گرفته و آن را روی سیستم **Windows** خود نصب می کند. کار نصب آن چندان هم آسان نیست. اول باید **Perl** را روی رایانه اش نصب کند و بعد **OpenSA** و در نهایت **Circumventor** را نصب کند. از این به بعد او باید همیشه کامپیوتر خود را روشن بگذارد تا سارا بتواند از آن به عنوان یک پروکسی شخصی استفاده کند. در غیر این صورت لازم خواهد بود تا هر بار که سارا می خواهد از پروکسی استفاده کند، او کامپیوترش را روشن کند. دوست سارا نرم افزار را آماده کرده، سپس با تلفن همراه سارا تماس می گیرد و **URL** ی را که سارا می تواند از طریق آن وارد سیستم پروکسی شود را به او می گوید. حالا سارا می تواند با استفاده از این آدرس در وب گشت بزند یا در وبلاگ خود مطلب بنویسد. این روش بسیار مطمئن است زیرا سارا می تواند از رایانه منزل یا کافی نت هم از این پروکسی شخصی استفاده کند و دیگر نیازی به تغییر چیزی در روی رایانه وجود ندارد.

در حالی که سارا بابت این کار از جیم بسیار متشکر است اما در مورد هماهنگی این مسئله یک مشکل وجود دارد. رایانه جیم - که از سیستم عامل ویندوز استفاده می کند همواره مشکل پیدا می کند و باید روشن و خاموش شود. هر وقت این اتفاق می افتد، سرویس دهنده اینترنت جیم یک **IP** جدید را به رایانه او اختصاص می دهد و در نتیجه هر بار که این جریان تکرار می شود، پروکسی شخصی از کار افتاده و سارا نمی تواند از آن استفاده کند. در این حالت جیم باید دوباره با سارا تماس گرفته و نشانی **IP** جدیدی را که **Circumventor** در حال کار بر روی آن است به سارا بدهد. این کار کم کم گران تمام شده و خسته کننده می شود. همچنین سارا هم نگران است که اگر از یک نشانی **IP** به مدت طولانی استفاده کند، ممکن است **ISP** او در مقابل فشار دولت تسلیم شده و آن را مسدود کند.

گام پنجم - Onion Routing از طریق TOR

جیم پیشنهاد می‌کند که سارا از Tor استفاده کند که سیستمی نسبتاً جدید و میزان گمنامی در آن بسیار بالاتر است. ایده Onion routing برگرفته از ایده پروکسی‌ها است - یعنی رایانه دیگری که به نفع شما کار می‌کند - ولی میزان پیچیدگی آن بسیار بیشتر است. هر درخواستی که از طریق شبکه Onion routing صورت می‌گیرد از دو الی بیست رایانه گذشته و همین مساله کار پیگیری کامپیوتری که در خواست اصلی از آن صورت گرفته است را بسیار دشوار می‌سازد. هر حلقه از زنجیره Onion routing رمزنگاری می‌شود و این مساله هم به نوبه خود کار را برای دولت سارا جهت پیگیری نوشته‌هایش سختتر می‌کند. علاوه بر این، هر رایانه حاضر در این زنجیره تنها نزدیکترین همسایگان خود را می‌شناسد. به عبارت دیگر، مسیریاب «ب» می‌داند که درخواست را از کامپیوتر «الف» گرفته است و باید این درخواست را به مسیریاب «ج» بفرستد. این درخواست رمزنگاری شده است و در نتیجه مسیریاب «ب» هیچ اطلاعی از این ندارد که سارا کدام صفحه را درخواست کرده و در نهایت کدام مسیریاب این صفحه را برای وی ارسال خواهد کرد.

با وجود پیچیدگی این فناوری، سارا در نهایت تعجب در می‌یابد که نصب Tor به عنوان یک سیستم Onion routing تا چه حد ساده است (<http://tor.eff.org/cvs/tor/doc/tor-doc-win32.html>). او یک برنامه نصب از اینترنت می‌گیرد که Tor را روی کامپیوترش نصب می‌کند. بعد برنامه نصب کننده Privoxy را از شبکه می‌گیرد و آن را نیز نصب می‌کند، این یک پروکسی است که به خوبی با Tor کار می‌کند و این قابلیت مثبت را هم دارد که بسیاری از تبلیغات ناخواسته را به شکل خودکار حذف می‌کند.

پس از نصب نرم افزار و راه اندازی مجدد دستگاه، سارا سری به noreply.org می‌زند و می‌بیند که برنامه Tor با موفقیت او را از دید دیگران مخفی کرده است چرا که noreply.org فکر می‌کند او از دانشگاه هاروارد به اینترنت وارد شده است. او صفحه را دوباره بارگذاری می‌کنند و می‌بینند که این بار سایت تصور می‌کند او از آلمان آمده است. سارا نتیجه می‌گیرد که با هر بار مراجعه به یک سایت، هویت جدیدی پیدا می‌کند و به این طریق تا حد زیادی ایمنی و خلوت‌اش حفظ می‌شود.

البته این کار پیامدهای عجیبی نیز دارد. وقتی که سارا از طریق Tor، در Google جستجو می‌کند، زبان گوگل دائماً تغییر می‌کند. یکی از جستجوها به انگلیسی - دیگری به ژاپنی، بعدی به آلمانی و بقیه به هلندی و دانمارکی انجام می‌شوند و تمام این اتفاقات در کمتر از چند دقیقه رخ می‌دهد. شاید این برای سارا فرصت خوبی باشد که با چند زبان آشنا شود ولی پیامدهای دیگری نیز وجود دارند.

سارا می‌خواهد از Wikipedia استفاده کند اما کشف می‌کند که Wikipedia تلاش او برای ویرایش مقالات را نادیده می‌گیرد.

به نظر می‌رسد که Tor نیز تا حدی دارای مشکلاتی همانند دیگر پروکسی‌ها است. زمان جستجو در حالی که Tor روشن است در مقایسه با زمان جستجوی معمولی تا حد زیادی افزایش یافته و پس از مدتی سارا به این نتیجه می‌رسد که تنها در زمان تلاش برای دسترسی به مطالب حساس یا درج چنین مطالبی در وبلاگ از Tor استفاده کند. از طرف دیگر در این روش سارا به کامپیوتر درون خانه‌اش وابسته است زیرا نصب نرم افزاری مانند Tor بر روی کافی‌نت‌ها عملاً غیر ممکن است.

چیزی که بیشتر او را نگران می‌سازد این است که Tor گاهی از کار می‌افتد. علاوه بر این به نظر می‌رسد که ISP او پس از مدتی دسترسی به برخی مسیریاب‌های Tor را مسدود کرده است و هنگامی که Tor سعی می‌کند از آن‌ها برای دسترسی به یک سایت مسدود شده استفاده کند، ممکن است چند دقیقه بگذرد و هیچ چیز روی صفحه نمایش داده نشود. در این مواقع سارا باید دگمه مربوط به بارگذاری مجدد را فشار دهد.

گام ششم - MIXMASTER ، INVISIBLOG و GPG

حتماً برای مشکل وبلاگ نویسی، راه حلی بدون استفاده از پروکسی هم وجود دارد حتی اگر به پیچیدگی Tor باشد. سارا پس از سر و کله زدن و بحث‌های فراوان با دوستان خیره کامپیوتر راه حل جدیدی می‌یابد: Invisiblog (<http://www.invisiblog.com>). این سرویس که از سوی یک گروه گمنام استرالیایی اداره می‌شود vigilant.tv نام دارد و سایتی است طراحی شده برای افراد واقعا محتاط. در این سیستم نمی‌توانید مانند یک وبلاگ معمولی، یعنی از طریق وب مطلب بنویسید. برای ارسال مطلب به invisiblog باید از ایمیلی استفاده کنید که توسط بازفرستنده MixMaster ارسال و با رمز امضا شده باشد.

سارا باید کمی تلاش می‌کرد تا جمله آخر را کامل درک کند. اول باید GPG را راه می‌انداخت (<http://www.gnupg.org/>) که پیاده‌سازی مبتنی بر GNU رمزگذاری Pretty Good Privacy است. (http://en.wikipedia.org/wiki/Public-key_cryptography).

در دو جمله: رمزگذاری کلید عمومی شیوه‌ای است که به سارا اجازه می‌دهد پیامی را برای کس دیگری بفرستد و تنها او قادر به خواندن آن‌ها باشد بدون اینکه لازم باشد کلیدی مخفی را برای آن فرد ارسال کند که به وی اجازه بدهد پیام‌هایی که دیگران برای سارا می‌فرستند را بخواند. رمزگذاری کلید عمومی همچنین به افراد اجازه می‌دهد تا سندی را امضای دیجیتالی کنند تا امکان جعل آن وجود نداشته باشد.

او یک «زوج کلید» ساخت تا بتواند با استفاده از آن‌ها در وبلاگ ایمن‌اش مطلب بنویسد. او مطالب را با «کلید خصوصی» امضا می‌کرد و بعد آن‌ها را برای سرویس دهنده ایمیل می‌کرد. از آنجایی که قبلاً «کلید عمومی» اش را در اختیار سرویس دهنده قرار داده بود، سرویس دهنده می‌توانست اولاً مطمئن شود که پیام‌ها از طرف او آمده‌اند و پس از کسب این اطمینان می‌توانست پیام‌های او را رمزگشایی کرده، آن‌ها را در وبلاگ قرار دهد. **(برای کسب اطلاعات بیشتر به بخش مربوط به اطمینان از ایمنی کامل پست الکترونیکی مراجعه نمایید).**

او سپس MixMaster را نصب کرد که یک سیستم ایمیل طراحی شده برای مخفی کردن مبدا ارسال نامه است. MixMaster از یک رشته ارسال کننده مجدد نامه گمنام استفاده می‌کند. یعنی از برنامه‌هایی که طراحی شده‌اند تا با حذف تمام اطلاعات مربوط به مبدا یک نامه و ارسال آن برای مقصد، ایمنی را تا حد ممکن بالا ببرند. با استفاده از رشته‌ای دو تا بیست زنجیره‌ای از این ارسال کننده‌های مجدد، ردگیری پیام‌های ارسالی عملاً غیر ممکن است حتی اگر یکی دو ارسال کننده مجدد هم در مقابل فشار دولت تسلیم شوند و اطلاعات را ذخیره و افشا کنند. سارا برای استفاده از MixMaster باید پس از دریافت سورس (منبع) منبع برنامه از اینترنت شخصاً آن را کمپایل کند؛ این احتیاج به کلی کمک از طرف یک نفر خیره کامپیوتر دارد.

او اولین پیام MixMaster را به Invisiblog ارسال می‌کند. این پیام شامل کلید عمومی اوست. سایت Invisiblog با استفاده از این کلید عمومی یک وبلاگ با نام بامزه invisiblog.com/ac4589d7001ac238 برای او ایجاد می‌کند. رشته عجیب بعد از invisiblog.com در حقیقت 16 حرف آخر کلمه عمومی سارا است. از این به بعد برای ارسال مطالب او باید اول مطلب خود را بنویسد، بعد از طریق کلید خصوصی‌اش آن را امضا کند و در نهایت با استفاده از MixMaster آن را برای Invisiblog بفرستند.

این روش، سرعت روش‌های قبلی را ندارد. راهنمایی‌های گمراه‌کننده MixMaster به این معنا است که رسیدن نامه به مقصد ممکن است چیزی بین دو ساعت تا دو روز طول بکشد. در عین حال او باید در سر زدن به وبلاگ احتیاط کند چرا که هر بار مشاهده او از این وبلاگ ممکن است در رایانه سرویس دهنده اینترنت ثبت شود و از این طریق دولت شک کند که او ممکن است نویسنده این وبلاگ باشد که اینقدر به آن سر می‌زند. اما نکته مثبت این است که او اطمینان دارد که مدیران Invisiblog هیچ ایده‌ای از هویت او ندارند.

مشکل اصلی این شیوه این است که استفاده از Invisiblog برای اکثر مردم مشکل است. نصب GPG برای آن‌ها یک چالش واقعی است و معمولاً برای درک مفهوم کلیدهای عمومی و خصوصی مشکل پیدا می‌کنند. البته ابزارهای خوش‌دستتری هم برای رمزگذاری GPG وجود دارند؛ مثلاً Ciphire. این برنامه‌ها به کسانی مثل سارا که مهارت‌های کامپیوتری کمتری دارند کمک می‌کنند تا با GPG کنار بیایند ولی کاربرد این برنامه‌ها هم با کمی ترفند همراه است. در نتیجه افراد بسیاری کمی - بخصوص از میان آن‌هایی که واقعاً نیازمند آن هستند - وجود دارند که بتوانند از رمزگذاری برای همه ایمیل‌هایشان استفاده کنند.

MixMaster برای اکثر افراد یک چالش فنی عمده است. کاربران ویندوزی باید نسخه قدیمی تحت DOS برنامه را از اینجا دریافت کنند: <http://prdownloads.sourceforge.net/mixmaer/mix204b46.zip?download> .. من آن را دریافت و آزمایش کردم ولی به نظر نمی‌رسید که درست کار کند... یا ممکن است ایمیل من هنوز در حال دست به دست شدن بین ارسال‌کننده‌های ناشناس مجدد باشد. اگر کسی بخواهد از نسخه جدیدتر استفاده کند یا برنامه را روی سیستم‌عامل‌های لینوکس یا مک استفاده کند باید شخصاً برنامه را کمپایل کند که حتی خیلی از کاربران حرفه‌ای هم توان آن را ندارند. در صورتی که Invisiblog این امکان را داشت که پیام‌های وبلاگ را از طریق ارسال‌کننده‌های مجدد تحت وب دریافت کند، کار بسیار آسان‌تر می‌شد ولی در حال حاضر من این سرویس را سرویس‌چندان مفیدی برای کسانی که واقعاً به آن احتیاج دارند، نمی‌بینم.

در کشورهای سرکوبگر، استفاده از رمزگذاری قوی یک مشکل دیگر هم ایجاد می‌کند. اگر رایانه سارا از سوی دولت ضبط و کلید خصوصی‌اش کشف شود، شاهی بسیار قوی علیه سارا خواهد بود که نشان می‌دهد او نویسنده مقالات مجادله برانگیز این وبلاگ بوده است. همچنین در کشورهایی که رمزنگاری استفاده زیادی ندارد، ارسال پیام از طریق MixMaster - یعنی ارسال ایمیلی که شدیداً رمزگذاری شده است - مشکوک بوده و ممکن است باعث بررسی دقیق‌تر فعالیت‌های سارا شود.

گمنامی تا چه حد لازم است؟ در این بحث تا کجا باید پیش رفت؟

آیا راه حلی که سارا پیدا کرده - یاد گرفتن رمزنگاری و نرم‌افزارهایی که بتواند از MixMaster استفاده کند - همان راه حل مورد نظر شما است؟ یا ترکیبی از گام‌های 1 تا 5 راه حل مورد نظر شما است؟ این سوال پاسخ مشخصی ندارد. روشی که قرار است برای مخفی سازی هویت شما به کار رود باید مبتنی بر شرایط منطقه‌ای، حوصله فنی شما و میزان علاقه شما به مخفی ماندن باشد. اگر فکر می‌کنید مطلبی که قرار است از طریق شما منتشر شود ممکن است برایتان ایجاد خطر کند، ارسال آن از طریق Tor بر روی یک وبلاگ تاسیس شده روی یک سرویس‌دهنده وبلاگ رایگان معمولاً راه حل مناسبی است.

و فراموش نکنید! نباید مطالب وبلاگ خود را با نام واقعی امضا کنید.

Ethan Zuckerman* یکی از افراد مرکز برکمان است که در زمینه اینترنت و جامعه در دانشکده حقوقی هاروارد فعالیت دارد و تمرکز تحقیقات وی بر روابط بین روزنامه‌نگاری شهروندان و رسانه‌های جمعی سنتی خصوصا در کشورهای در حال توسعه است. او بنیانگذار و رئیس سابق *Geekcorps* است که سازمانی غیرانتفاعی است و در زمینه آموزش فناوری در کشورهای در حال توسعه فعالیت می‌کند. او همچنین یکی از بنیانگذاران شرکت میزبانی وب *Tripod* نیز هست.



شیوه های فنی برای دور زدن سانسور

*نوشته نارت ویلنیو

فهرست مطالب

- فیلتر گذاری محتوای اینترنت
- فن آوری دور زدن فیلتر
- تعیین نیازها و ظرفیت ها
- دور زننده های تحت وب
- سرویس های دور زدن تحت وب عمومی
- نرم افزار دور زدن مبتنی بر وب
- مسائل امنیتی مرتبط با دور زننده های تحت وب
- سرویس های پروکسی
- نرم افزار پروکسی سرور
- پروکسی سرورهای قابل دسترسی عمومی
- یافتن پروکسی های باز
- مسائل امنیتی مرتبط با پروکسی سرورها
- تونل زدن
- سیستم های ارتباطی گمنام

نتیجه گیری

فیلتر گذاری محتوای اینترنت

فن آوری فیلترگذاری امکان کنترل دسترسی به محتوای اینترنت را فراهم می‌کند. اگرچه تمرکز این فن آوری‌ها در مقطع ابتدایی بر روی کنترل دسترسی افراد بوده است تا به والدین اجازه دهد دسترسی کودکان به محتوای نامناسب را محدود کنند اما امروزه، فن آوری فیلترگذاری به طور گسترده و در سطح موسسات و سازمان‌ها بکار گرفته می‌شود. کنترل دسترسی به محتوای اینترنت در حال حاضر در بعضی از موسسات از جمله مدارس، کتابخانه‌ها و شرکت‌های بزرگ در اولویت قرار گرفته است؛ همچنین این روزها فیلترکردن اینترنت در چند کشور هم دیده می‌شود. در این کشورها دسترسی به محتوای اینترنت برای کل جمعیت کشور ناممکن می‌شود بدون اینکه کسی پاسخگو باشد.

فن‌آوری‌های فیلترگذاری عموماً مبتنی بر یک فهرست از سایت‌های مسدود شده هستند که گاهی با فیلترکردن یکسری کلمات خاص همراه می‌شوند تا بتوانند به شکل پویا محتوای اینترنت را سانسور کنند. در این روش فهرستی از URLها و نام «دومین»های مورد نظر ایجاد و بعد وارد نرم‌افزار فیلترینگ می‌شود که قابلیت سانسور طبقه‌بندی‌های مختلف را دارد. وقتی قرار است کسی به سایتی متصل شود، نرم‌افزار فیلترینگ سایت مورد نظر را با فهرست سایت‌های فیلتر شده مقایسه می‌کند و در صورتی که با آن منطبق باشد، اجازه دسترسی به آن را نمی‌دهد. علاوه بر این اگر فیلتر مبتنی بر کلمات هم فعال شده باشد، نرم‌افزار هر صفحه (یعنی نام دامنه، URL و تمام چیزهای بعد از / و حتی گاهی محتویات درون صفحه) را از نظر داشتن این کلمات بررسی می‌کند و در صورت وجود عبارات نامطلوب، به شکل پویا دسترسی به سایت را غیرممکن می‌کند.

سیستم‌های فیلترگذاری ماهیتاً دارای دو نقص هستند: مسدود کردن بیش از حد و مسدود کردن کمتر از حد. این برنامه‌ها همیشه بعضی صفحات را به اشتباه سانسور می‌کنند و همیشه صفحاتی هستند که از نظر تولید کنندگان نرم‌افزار باید سانسور شوند ولی از زیر دست برنامه جان سالم به در می‌برند. البته کلید اصلی پنهان در پشت نرم‌افزارهای فیلترینگ، شیوه ایجاد فهرست سایت‌های ممنوعه است. اگر چه فهرست‌های رایگان هم وجود دارند (که تمرکز بیشتر آنها بر هزینه نگاری است)، فهرست برنامه‌های فیلترگذاری تجاری و فهرست‌هایی که در سطح ملی به کار گرفته می‌شوند، همواره سری باقی می‌مانند. فهرست‌های تجاری مربوط به طبقه‌بندی سایت‌های مسدود شده، تحت مالکیت معنوی ایجاد کنندگان آنها هستند و هرگز در اختیار عموم قرار نمی‌گیرند. علی‌رغم این که سازندگان برخی نرم‌افزارهای فیلترگذاری امکان بررسی On line فیلتر بودن یا نبودن URLها را فراهم می‌کنند؛ کلیت فهرست سایت‌های فیلتر شده جزو اسرار به حساب می‌آیند و برای تحلیل یا موشکافی در اختیار عموم مردم قرار نمی‌گیرند.

حتی کشورهای فیلترکننده اینترنتی که از نرم‌افزارهای تجاری استفاده می‌کنند هم نام سایت‌های بسیاری را برای مسدود شدن به فهرست اصلی اضافه می‌کنند. این سایت‌های مسدود شده معمولاً متعلق به احزاب سیاسی مخالف یا روزنامه‌ها، سازمان‌های حقوق بشری، ارائه دهندگان اخبار بین‌المللی و متون انتقادی علیه دولت هستند. کشورهای سانسورگر معمولاً تمرکز بیشتری بر محتویاتی دارند که به زبان محلی آن کشور نوشته شده است، مانند وبلاگ‌ها و انجمن‌های بحث و گفت و گو و در مورد سایت‌های انگلیسی زبان چندان سخت نمی‌گیرند.

فن آوری‌های دور زدن فیلتر

در پاسخ به فیلترگذاری اینترنتی از سوی دولت و رژیم هایی که کنترل سخت را اعمال می کنند، فن‌آوری‌های بسیاری برای دور زدن فیلتر ایجاد شده‌اند که به کاربران اجازه می‌دهند از فیلترها عبور کنند. پروژه‌های بسیاری وجود دارند که هدفشان توسعه فن‌آوری‌هایی است که به شهروندان و شبکه جامعه مدنی اجازه دهد خود را در برابر سانسور و نظارت اینترنت مجهز کنند یا آن‌ها را دور بزنند. این ابزارها را «فن‌آوری دور زدن» می‌نامند. به طور کلی، فن‌آوری‌های دور زدن بر اساس این کار می‌کنند که کامپیوتری در جایی آزاد از جهان اطلاعات بین کامپیوتر سانسور شده و اطلاعات مورد نظر نقش میانجی را بازی می‌کند. این رایانه واسط، متون درخواستی کاربر را از مقصد دریافت کرده و آن را برای وی ارسال می‌کند. گاهی اوقات، ممکن است این فن‌آوری‌ها برای پاسخگویی به شرایط خاص فیلترینگ یک کشور طراحی یا تنظیم شده باشند. در مواقع دیگر، کاربران به راحتی می‌توانند تکنولوژی‌های موجود را برای دور زدن فیلتر تنظیم کنند؛ حتی اگر آن تکنولوژی‌ها برای این منظور طراحی نشده باشند.

برخی از این فن‌آوری‌ها توسط شرکت‌های خصوصی طراحی شده است و برخی دیگر نیز توسط هکرها و فعالان اجتماعی. طیف آنها بسیار گسترده است و برنامه‌های کوچک و ساده تا برنامه‌های پیچیده مبتنی بر پروتکل نقطه به نقطه را شامل می‌شود. با توجه به طیف وسیع فن‌آوری‌های موجود، کاربران احتمالی باید بتوانند نقاط قوت و ضعف هر کدام از آن‌ها را بسنجند تا قادر باشند مناسبترین فن‌آوری دور زدن را مطابق نیاز خود انتخاب کنند.

فن‌آوری دور زدن دو دسته کاربر دارد: شخصی که این خدمات را ارائه می‌دهد و شخصی که از آن استفاده می‌کند. رایانه دهنده خدمات، نرم افزار را روی رایانه‌ای که در محیطی بدون فیلتر قرار دارد نصب می‌کند و خدمات آن را در اختیار کسانی قرار می‌دهد که از مناطق دارای سانسور به اینترنت وصل می‌شوند. بنابراین داشتن یک سیستم دور زننده موفق، در گرو پاسخگویی به نیازهای هر دو دسته کاربران است.

هدف این مقاله اطلاع رسانی به کاربرانی است که تصمیم‌گرفته‌اند از فن‌آوری‌های دور زدن موجود استفاده کنند و تلاش می‌کند نحوه ارزیابی انتخاب‌های موجود برای یافتن بهترین راه حل را در اختیار آن‌ها قرار دهد. این کار از طریق تشخیص نیازها و ظرفیت‌های کاربران - هم آنانی که سرویس‌ها را آماده می‌کنند و هم آنانی که آن را استفاده می‌کنند - در حین ایجاد توازن مناسب بین قابلیت استفاده تکنولوژی توسط کاربران غیرحرفه‌ای و ایمنی حاصله است. دور زدن موثر، ایمن و پایدار از طریق تطبیق فن‌آوری درست با کاربر درست به دست می‌آید.

تعیین نیازها و ظرفیت ها

فن‌آوری‌های دور زدن اغلب دارای گروه هدف وسیعی هستند از جمله کاربران با منابع و سطوح مهارت متفاوت. چیزی که ممکن است تحت یک سناریو به خوبی پاسخگو باشد، ممکن است در شرایطی دیگر انتخاب خوبی نباشد. در زمان انتخاب فن‌آوری دور زدن رایج کنندگان و کاربران آن باید به این سوالات پاسخ دهند:

تعداد کاربران احتمالی و پهنای باند موجود چیست؟ (برای ارائه کننده و کاربر فن‌آوری دور زدن)
اصلی‌ترین محل اتصال کجاست و هدف آن‌ها از استفاده از اینترنت چیست؟
سطح مهارت های فنی آنها چقدر است؟ (برای ارائه کننده و کاربر فن‌آوری دور زدن)
کاربر نهایی چه رابط‌های قابل اعتمادی در خارج از کشور دارد؟
مجازت احتمالی کاربرانی که در حین استفاده از فن‌آوری دور زدن گیر بیافتند، چیست؟
آیا کاربر نهایی به درستی از خطرات امنیتی همراه با استفاده از فن‌آوری‌های دور زدن آگاه است؟

تعداد کاربران و پهنای باند موجود

ارائه کننده سیستم‌های دور زدن باید تعداد کاربرانی که این فن‌آوری قرار است تحت پوشش دهد را تخمین زده و آن را با پهنای باند قابل استفاده‌شان متوازن نماید. کاربر نهایی نیز باید نسبت به پهنای باند مصرفی خود آگاهی داشته باشد چرا که استفاده از دور زننده‌ها ارتباط را کند می‌کند.

افرادی که علاقه مند به برپایی پروکسی‌های عمومی هستند باید در نظر داشته باشند که دورزننده آنها ممکن است از سوی افرادی خارج از مناطق تحت سانسور نیز مورد استفاده قرار بگیرد. به عنوان مثال، ممکن است از دورزننده برای دریافت کل یک فیلم از شبکه استفاده شود و به این ترتیب پهنای باند بسیاری اشغال شود. بنابراین، ممکن است بخواهید دسترسی به دورزننده خود یا میزان پهنای باند مجاز در هنگام استفاده از آن را محدود نمایید. فن‌آوری‌های مختلف موجود، برخی یا همه این گزینه‌ها را در اختیار شما قرار می‌دهند.

حل اصلی اتصال و استفاده

بر اساس اینکه کاربران نهایی قرار است از چه محلی به اینترنت متصل شوند و می‌خواهند از طریق دور زننده چه کارهایی بکنند، گزینه‌های مختلفی در پیش رو خواهد بود.

به عنوان مثال، کاربرانی که با استفاه از رایانه های عمومی یا کافینتها به اینترنت متصل می‌شوند، قادر به نصب هیچ گونه نرم افزاری نبوده و محدود به راه حل‌های تحت وب هستند. این احتمال هم وجود دارد که برخی از کاربران بخواهند علاوه بر گشت زنی در وب (HTTP) از سرویس‌های دیگری همچون ایمیل (SMTP) و انتقال فایل (FTP) هم استفاده کنند که در این صورت باید بتوانند نرم افزارهای مختلفی را روی کامپیوترهای خود نصب کنند و بر روی آن‌ها تنظیماتی را تغییر دهند. مشخص است که این مساله نیازمند مهارت‌های بیشتری از سوی کاربر است.

سطح مهارت های فنی

هر چه سطح دانش و مهارت فنی کاربران بالاتر باشد (و به نسبت آن تعداد کاربران کمتر) گزینه‌های قابل اجرا در دوزننده‌ها بیشتر می‌شود. موانع پیش روی کاربران غیر فنی شامل نصب و راه اندازی برنامه‌ها و همچنین اجرای تنظیمات و بعضی تغییراتی است که لازم است هنگام استفاده از فن‌آوری دوزننده صورت گیرد. این مساله هم در مورد ارایه کننده سرویس صادق است و هم استفاده کننده آن. استفاده نادرست از فن‌آوری دور زدن می تواند کاربران را با خطرات اجتناب ناپذیر رو در رو کند.

وجود رابط‌های قابل اعتماد

کاربر نهایی در صورتی که فردی قابل اطمینان در خارج از کشور را بشناسد، می‌تواند گزینه‌های دور زدن سانسور خود را بسیار افزایش دهد. اگر کاربر، رابط قابل اطمینانی در خارج از کشور نداشته باشد، گزینه‌های محدود به سیستم‌های عمومی موجود خواهد بود و وقتی کاربر قادر به شناسایی و استفاده از این امکانات است، پس فیلترگذاران هم می‌توانند آن‌ها را پیدا و مسدود کنند. با داشتن رابطی قابل اطمینان، کاربر نهایی می تواند با سرویس دهنده دوزننده در تماس باشد و راه حلی پیدا کند که دقیقاً پاسخگوی شرایط موجود بوده و برای جلوگیری از کشف و مسدود شدن، بتوان آن را خصوصی نگه داشت. با داشتن یک رابط قابل اعتماد در کشوری بدون سانسور امکان دور زدن سانسور به شکل موفق، طولانی مدت و پایدار بسیار افزایش می‌یابد.

مجازات احتمالی

دانستن مجازات احتمالی که کاربران در صورت گیر افتادن حین استفاده از دوزننده‌ها با آن مواجه خواهند شد نیز اهمیت بسیاری دارد. با توجه به جدیت موضوع، گزینه‌ها متفاوت خواهند بود. اگر نظام حقوقی نسبت به این موضوع بی‌اعتنا بوده و مجازات احتمالی ناچیز باشد، کاربر می‌تواند از بین گزینه‌های مختلف آنهایی را انتخاب کند که از ایمنی بالایی برخوردار نبوده اما دوزننده‌های موثری هستند. اگر شرایط بسیار خطرناک باشد، باید فن‌آوری‌هایی انتخاب شوند که ایمن و کم‌خطرتر هستند.

در عین حال ممکن است بتوان از بعضی برنامه‌ها زیر پوشش‌های قانونی استفاده کرد یا به شکلی دیگر هدف اصلی آن‌ها را مخفی نمود.

خطرات امنیتی

زیاد پیش می‌آید که کاربران تشویق به استفاده از فن‌آوری‌های دور زننده می‌شوند بدون این که خطرات احتمالی اینکار به آن‌ها گوشزد شود. در حالی که در صورت استفاده از تکنولوژی صحیح، در مکان و زمان صحیح و توسط فرد صحیح می‌توان این خطرات را به حداقل رساند.



دورزننده‌های تحت وب

دورزننده‌های تحت وب صفحات خاصی در وب هستند که با داشتن یک فرم به کاربران اجازه می‌دهند، به سادگی URL مورد نظر خود را در آن وارد کنند و وظیفه دریافت آن صفحه و نشان دادن آن به کاربر را بر عهده دورزننده تحت وب بگذارند. در این حالت هیچ اتصال مستقیمی بین کاربر و وبسایت مورد تقاضا وجود ندارد و دور زننده بدون اینکه دیده شود، مانند یک پروکسی عمل می‌کند که به کاربر اجازه می‌دهد، بدون هیچ ردپایی در شبکه مسدود شده گشت بزند. دورزننده‌های تحت وب به شکل خودکار تمام پیوندهای درون صفحات را به شکلی به سمت دورزننده تغییر جهت می‌دهند که کاربر بدون احساس ناراحتی بتواند در سایت سانسور شده گشت‌زنی کند.



در هنگام استفاده از دورزننده‌های تحت وب، کاربر نهایی نیازی به نصب نرم‌افزار یا تغییر تنظیمات مرورگر خود ندارد. تنها کاری که کاربر نهایی باید انجام دهد، رفتن به URL این دورزننده و وارد نمودن URL مورد تقاضا در صفحه آن و در نهایت فشردن دکمه ارسال است (دورزننده‌های تحت وب شاید در ظاهر با هم متفاوت باشند ولی عملکرد اولیه آنها یکسان است). در نتیجه به سطح خاصی از مهارت نیاز نیست و از هر جایی هم می‌توان از این سیستم‌ها استفاده کرد.

مزایا :

دورزننده‌های تحت وب، سیستم ساده‌ای دارند و استفاده از آنها نیز آسان است و کاربر نهایی نیازی به نصب هیچ نرم‌افزاری ندارد. کاربرانی که رابط قابل اطمینانی در خارج ندارند نیز می‌توانند از خدمات دورزننده‌های عمومی تحت وب استفاده کنند. سیستم‌های دورزننده تحت وب شخصی را می‌توان طوری تنظیم کرد که پاسخگوی نیازهای کاربران در شرایط خاص باشد و مقامات فیلترگذار نیز کمتر قادر به یافتن آنها خواهند بود.

معایب:

سیستم‌های دورزننده تحت وب عموماً محدود به ترافیک وب (HTTP) بوده و معمولاً به شکل رمزگذاری شده (SSL) قابل دسترسی نیستند. همچنین سرویس‌های تحت وب (مثلاً ایمیل تحت وب) که نیازمند ورود به شبکه باشند نیز معمولاً در این روش قابل دسترسی نخواهند بود. سرویس‌های دورزننده تحت وب عمومی معمولاً به خوبی شناخته شده‌اند و ممکن است از سوی مقامات مسدود شده باشند. در حال حاضر اکثر این سرویس‌دهندگان توسط نرم‌افزارهای فیلترگذاری تجاری مسدود شده‌اند.

سیستم‌های شخصی دورزننده تحت وب نیاز به همکاری یک نفر قابل اعتماد در منطقه‌ای فیلتر نشده دارند. در حالت ایده‌آل، هر دو طرف باید بتوانند به شیوه‌ای با یکدیگر ارتباط برقرار کنند که به آسانی قابل نظارت و پیگیری نباشد.

خدمات دورزننده مبتنی بر وب عمومی

نرم‌افزار و سرویس‌های عمومی دورزننده بسیاری در اینترنت وجود دارند. بیشتر آنها خدمات خود را مجانی ارائه می‌دهند ولی بعضی نیز برای گزینه‌های متنوع‌تری همچون دسترسی رمزگذاری شده پول درخواست می‌کنند. بعضی از این سرویس‌ها توسط شرکت‌ها اداره می‌شوند در حالی که بعضی دیگر به عنوان یک سرویس عمومی و توسط داوطلبان اداره می‌شوند. به عنوان مثال:

<http://www.anonymizer.com>

<http://www.unipeak.com>

<http://www.anonymizer.ws>

<http://www.proxyweb.net>

<http://www.guardster.com>

<http://www.webwarper.net>

<http://www.proximal.com>

<http://www.the-cloak.com>

از آنجایی که این سایتها در همه جا شناخته شده هستند، اکثر نرم افزارهای فیلترگذاری تجاری و همچنین اکثر کشورهای فیلتر کننده اینترنت در حال حاضر آنها را در فهرست سایتهای فیلتر شده قرار داده اند. اگر آدرس این سایتها در فهرست باشند، نمی توانید از سرویسهای آنان استفاده کنید. همچنین بسیاری از سرویس دهندگان عمومی دورزننده ها، ترافیک ارسالی به کاربر نهایی را رمزگذاری نمی کنند. پس این احتمال وجود دارد که داده هایی که برای این سرویس دهنددها ارسال یا از آنها دریافت می شود، توسط افراد مسولین دورزننده ها شنود شوند.³

استفاده از دورزننده های عمومی تحت وب برای کاربرانی مناسب است که در شرایط کم خطر کار می کنند و آشنای قابل اعتمادی در نقاط بدون سانسور ندارند و تنها می خواهند به شکل موردی و موقت از فیلتر عبور کنند و به دنبال ارسال یا دریافت اطلاعات حساس نیز نیستند.

نرم افزار دورزننده تحت وب

نصب نرم افزارهای دورزننده تحت وب ممکن است نیاز به مهارت فنی و منابع مناسب (مانند یک سرویس دهنده وب و پهنای باند) باشد. با استفاده از دورزننده های خصوصی، محل دورزننده فقط در اختیار استفاده کنندگان آن باقی می ماند در حالی که در صورت استفاده از دورزننده های عمومی، هم کاربران به آدرس آن دسترسی دارند و هم مسولین فیلترگذاری (و در عین حال اکثر نرم افزارهای تجاری فیلترگذاری نیز این آدرسها در فهرست سانسور خود قرار داده اند). احتمال ردیابی، کشف و بسته شدن دورزننده های تحت وب خصوصی بسیار کمتر از سرویس دهنددهای عمومی است.

دورزننده خصوصی را می توان با کمی تغییر برای کار در شرایط مختلف آماده کرد. برخی از تنظیمات معمول عبارت هستند از تغییر پورتی که دورزننده روی آن کار می کند و اضافه کردن رمزگذاری. **Secure Sockets Layer** یا **SSL** پروتکلی است که توسط آن اطلاعات رمزگذاری شده در اینترنت منتقل می شوند.

³ لازم به توجه است که اگر دورزننده ای از رمزگذاری استفاده نکند، دولت نیز خواهد توانست اطلاعات دریافتی و ارسالی آن را شنود کند. همچنین در این صورت این امکان برای دولت وجود دارد که کشف کند چه کسی با استفاده از کدام دورزننده به چه سایتی سر زده است.

این قابلیت عموماً از سوی سایتها برای تبادل ایمن اطلاعاتی چون شماره کارت‌های اعتباری استفاده می‌شود. برای دسترسی به سایت‌های که از SSL استفاده می‌کند لازم است به جای HTTP از HTTPS استفاده شود.

یکی دیگر از جاهایی که SSL کاربرد دارد، ایجاد یک سایت معمولی و پنهان کردن برنامه دور زننده در یک شاخه آن است که اسمی اتفاقی دارد. اگرچه مسوول بررسی می‌تواند ببیند که شما به چه سرویس دهنده‌ای متصل شده‌اید قادر نخواهد بود صفحه مورد بازدید شما را مشخص کند چون این بخش از سایت رمزگذاری شده است. برای مثال اگر یک نفر به <https://example.com/secretcircumventor/> متصل شود، مسوول بازرسی دسترسی‌ها می‌تواند مشخص کند که او به سایت example.com وصل شده اما هرگز نمی‌تواند کشف کند که او از یک دورزننده استفاده کرده است. اگر مسوول این سایت یک صفحه بی‌ضرر را در example.com قرار دهد، حتی در صورت مراجعه ناظر به این سایت هم وجود دورزننده لو نخواهد رفت.

- CGIProxy: یک برنامه CGI است که مانند یک پروکسی HTTP یا FTP کار می‌کند. <http://www.jmarshall.com/tools/cgiproxy>
- دور زننده Peacefire: برنامه خودکاری که نصب و راه اندازی CGIProxy را برای افراد غیر فنی بسیار ساده می‌کند: <http://www.peacefire.org/circumventor/simple-circumventor-instructions.html>
- pHProxy: یک دورزننده آزمایشی و بسیار قابل تنظیم تحت وب: <http://ice.citizenlab.org/projects/phproxy>
- Pshiphon: وب سرور با قابلیت SSL با یک دور زننده تحت وب داخلی. آدرس آن به زودی ارائه خواهد شد.

دورزننده‌های تحت وب خصوصی، با رمزگذاری فعال شده بهترین ابزار برای کاربرانی هستند که نیازمند خدمات دورزننده پایدار بوده و به یک رابط قابل اطمینان در مناطق بدون سانسور دسترسی دارند که مهارت‌های فنی کافی و دسترسی به پهنای باند مناسب برای نصب یک دورزننده تحت وب را داشته باشد. این انعطاف پذیرترین گزینه ایجاد دورزننده‌ها برای کارهای معمول تحت وب است و احتمال بسیاری کمی دارد که کشف و بسته شود.

مسائل امنیتی مرتبط با دورزننده‌های تحت وب

سیستم های دورزننده الزاما گمنامی را تضمین نمی‌کنند. البته هویت اصلی کاربر از دید مدیران سایت‌هایی که کاربر بازدید کرده است مخفی می‌ماند ولی در صورتی که ارتباط بین کاربر و سیستم دور زننده متن ساده (HTTP) باشد (که در مورد سرویس‌های رایگان معمولا اینگونه است) فرد بازرسی کننده (مثلا مسوول ISP) می‌تواند آن را شنود و تحلیل کند. در این صورت، هرچند که دورزدن موفق بوده است، مسوولان هنوز قادر هستند ردپاها را پیگیری و کشف کنند که کاربر با یک سیستم دورزننده کار کرده است. حتی این امکان هم وجود دارد که پیدا کنند به چه وبسایت‌هایی سر زده‌اید، در آن‌ها چه کار کرده‌اید و چه چیزی رد و بدل نموده‌اید.

دورزننده‌های تحت وبی که در حالت متن ساده (رمزگذاری نشده) کار می‌کنند گاهی از سیستم‌های مبهم کننده URL استفاده می‌کنند تا با سانسور مبتنی بر وجود کلماتی خاص در نام دامنه مبارزه کنند. برای مثال با استفاده از یک تکنیک ساده مانند ROT-13 که در آن هر حرف، 13 حرف جلوتر حرکت می‌کند، آدرس <http://ice.citizenlab.org> تبدیل به uggc://vpr.pvgvmrayno.bet می‌شود. در حقیقت، متن URL رمزنگاری می‌شود تا کلمات کلیدی ذکر شده در فهرست‌های فیلترگذاری در آن ظاهر نشوند. در این وضعیت با وجودی که دورزدن موفقیت‌آمیز بوده است، محتوای ارتباط همچنان قابل پیگیری است.

همچنین خطراتی در استفاده از کوکی‌ها و برنامه‌ها هم وجود دارد. بسیاری از دورزننده‌ها را می‌توان به شکلی تنظیم کرد که از کوکی‌ها و برنامه‌ها استفاده نکنند ولی در این حالت بسیاری از سایت‌ها (مثلا ایمیل‌های تحت وب) غیرقابل استفاده می‌شوند. به هنگام فعال کردن این گزینه‌ها باید با دقت عمل کرد. خطر دیگری که در این زمینه خصوصا در زمان استفاده از خدمات نیازمند Login وجود دارد، دسترسی به دورزننده‌ها از طریق ارتباط متنی ساده و سپس استفاده از آنها برای دریافت اطلاعات از یک رایانه کننده خدمات رمزنگاری شده است. در این شرایط، دورزننده اطلاعات تقاضا شده را از طریق SSL به شکل رمزگذاری شده دریافت می‌کند ولی بعد آن را بدون رمزگذاری بر روی خط ارتباطی کاربر قرار می‌دهد که در این وضعیت احتمال شنود آن‌ها و فاش شدن اطلاعات حساس بسیار بالا است.

برخی از این مسائل امنیتی را می‌توان با استفاده از پروکسی‌های تحت وب بر روی یک ارتباط رمزگذاری شده حل کرد. بعضی از پروکسی‌های تحت وب به شکلی تنظیم شده‌اند که می‌توانند تقاضاهای SSL یا همان HTTPS را قبول کنند که رابطه بی‌کاربر نهایی و دورزننده را رمزگذاری می‌کنند. در این حالت، کسی که در حال بررسی دسترسی‌ها است حداکثر می‌تواند متوجه شود که افراد در حال استفاده از دورزننده‌های رمزگذاری شده هستند ولی درباره این موضوع که آن‌ها دقیقا مشغول چه کاری هستند، چیزی دستگیرش نخواهد شد. شیدا پیشنهاد می‌شود که در صورت بالا بودن حساسیت کار، کاربران از دورزننده‌های تحت وبی استفاده کنند که SSL آنها فعال شده باشد.

در عین حال، اگر چه ممکن است ارتباط کاربر نهایی با دورزننده تحت وب ایمن باشد، ولی هر گونه اطلاعاتی که از طریق دورزننده تحت وب مبادله شود می‌تواند توسط مدیر دورزننده مشاهده شود. یک مشکل امنیتی دیگر اطلاعاتی است که رایبه کننده خدمات دورزننده ثبت می‌کند. بسته به محل دورزننده یا محل سرویس‌دهنده آن‌ها، این احتمال وجود دارد که مقامات بتوانند به سوابق کاری افراد دسترسی پیدا کنند.

حتی زمانی که افراد از دورزننده‌های تحت وب با SSL فعال استفاده می‌کنند، برخی مسائل حل نشده باقی می‌مانند که کاربران باید از آن‌ها آگاه باشند. یکی از این مسائل این است که استفاده از رمزنگاری ممکن است توجه بیشتری را به سوی فعالیت‌های دورزننده کاربر نهایی جلب کرده و همچنین رمزنگاری ممکن است در بعضی نقاط جهان قانونی نباشد. همچنین ممکن است مقامات مسئول فیلترگذاری حتی در صورت استفاده از SSL نیز با استفاده از شیوه‌هایی مثل «اثرانگشت SSL» و حمله‌های «آدم در وسط (MITM)» بتوانند تعیین کنند که کاربر نهایی از طریق دورزننده‌های تحت وب از چه سایت‌هایی بازدید کرده است. البته صفحاتی با متون پویا یا دورزننده‌هایی که متون و عکس‌های گمراه کننده را به صفحه مورد تقاضا اضافه می‌کنند می‌تواند احتمال این امر را کم کنند تا جایی که عملاً خطری نداشته باشد. اگر کاربران بتوانند از «انگشت نگاری» یا امضای ایمن سند SSL برخوردار شوند، این امکان برایشان به وجود می‌آید که شخصاً صحت و اعتبار صفحه دریافت شده را بررسی کنند و در نتیجه در مقابل حملات «آدم در وسط» ایمن شوند.⁴



پروکسی سرورها

«پروکسی سرور» سرویس دهنده ای است که بین یک سرویس‌گیرنده (مثلاً مرورگر وب) و سرویس‌دهنده (مثلاً وبسایت) واسط می‌شود. پروکسی سرور مانند یک حافظه میاجی (بافر) بین مشتری و سرویس‌دهنده عمل می‌کند و می‌تواند از انواع مختلف شیوه‌های ارتباطی شامل وب (HTTP)، انتقال فایل (FTP) و تبادلات رمزنگاری شده (SSL) پشتیبانی کند.

⁴ برای کسب اطلاعات بیشتر در زمینه حملات به دورزننده‌های تحت وب به مقاله بنت هسلتون مراجعه نمایید (فهرست ضعف‌های احتمالی سیستم دورزننده فیلترهای اینترنتی) در

و پاسخ پل بارانوسکی در <http://peacefire.org/circumventor/list-of-possible-weaknesses.html> و www.peek-a-booty.org/pbhtml/downloads/ResponseToLopwisticic.pdf

پروکسی سرورها توسط افراد، موسسات و دولت ها برای اهداف گوناگونی چون امنیت، گمنامی، افزایش سرعت و حتی فیلترگذاری مورد استفاده قرار می‌گیرد. برای استفاده از پروکسی سرور، کاربر نهایی باید در تنظیمات مرورگر خود تغییراتی انجام دهد و نشانی IP یا نام میزبان پروکسی سرور و همچنین شماره پورت یا درگاه مورد استفاده پروکسی سرور را وارد کند. هرچند که این کار بسیار ساده به نظر می‌رسد ولی ممکن است در مکان‌های عمومی مانند کتابخانه‌ها، کافی‌نت‌ها و یا حتی محل کار امکان‌پذیر نباشد.

مزایا :

بسته‌های نرم‌افزاری مختلفی وجود دارند که می‌توان توسط آن‌ها پروکسی‌های نامرئی راه انداخت که علاوه بر وب (HTTP) ارتباطات دیگر را نیز کنترل کنند. همچنین در این برنامه‌ها امکان استفاده از پورت‌های غیر استاندارد هم وجود دارد. پروکسی‌سرورهای رایگان و عمومی بسیاری هم در وب قابل پیدا کردن هستند.

معایب:

بسیاری از پروکسی سرورها به شکل پیش‌فرض از رمزنگاری استفاده نمی‌کنند و در نتیجه تبادل اطلاعات بین پروکسی و کاربر ایمن نیست. کاربر باید مجوزهای لازم برای تغییر تنظیمات مرورگر را داشته باشد و اگر ISPها طوری تنظیم شوند که همه ترافیک را مجبور به گذشتن از پروکسی‌ای خاص کنند، امکان استفاده از پروکسی سرورهای آزاد وجود نخواهد داشت. جستجو به دنبال پروکسی سرورهای باز و استفاده از آن‌ها ممکن است غیرقانونی باشد و همچنین این پروکسی‌ها ممکن است در هر لحظه‌ای قطع شوند.

نرم افزارهای پروکسی سرور

نرم‌افزارهای پروکسی سرور را می‌توان با کمک رابطین مورد اطمینان دارای مهارت‌های فنی لازم در خارج از کشوری که تحت فیلتر قرار دارد، روی سرور نصب کرد. نرم افزار پروکسی سرور باید در جایی نصب شود که پهنای باند کافی وجود داشته باشد و همچنین باید گزینه رمزگذاری آن را فعال کرد. استفاده از این روش در سازمان‌ها و دفاتر کوچکی که نیاز به دور زنده‌های پایدار دارند، راه حل مناسبی است. کاربران بعد از اینکه تنظیمات لازم برای استفاده از پروکسی‌سرور را در مرورگرهای خود انجام دادند، می‌توانند آزادانه و شفاف در اینترنت گشت بزنند. پروکسی سرورها پنهان‌ترین راه دور زدن فیلتر نیستند اما در مقایسه با سیستم‌های مبتنی بر وب، بسیار قرص و محکم‌ترند. پروکسی سرورها در مقایسه با پروکسی‌های تحت وب این مزیت را دارند که می‌شود از آن‌ها برای ورود به سایت‌هایی که نیازمند کوکی‌ها و لاگین هستند (مانند سیستم‌های ایمیل تحت وب) نیز استفاده کرد.

همچنین پروکسی سرورها را می توان به گونه ای تنظیم کرد که پاسخگوی نیازهای سیستم های فیلترگذاری محیط های خاص باشند.

- Squid یک نرم افزار پروکسی سرور است که می توان توسط Stunnel آن را ایمن کرد.
<http://www.squid-cache.org>
<http://www.stunnel.org>
<http://ice.citizenlab.org/projects/aardvark>
- Privoxy یک پروکسی با توانایی های فیلترگذاری بالا است که می تواند از حوزه شخصی شما محافظت کند.
<http://www.privoxy.org>
- Secure Shell یا SSH دارای یک socks proxy داخلی است
\$ssh - D port secure.host.com
<http://www.openssh.com>
- HTTPport/HTTPhost به شما اجازه می دهد تا از پروکسی HTTP که دسترسی اینترنت شما را مسدود می کند، رد شوید.

پروکسی سرور های شخصی با قابلیت رمزنگاری بهترین شیوه برای گروه ها و کاربرانی هستند که در محیطی اداری به یک دورزننده دائمی و پایدار نیاز داشته و همچنین به رابط قابل اعتمادی که دارای مهارت های فنی کافی برای نصب و نگهداری یک پروکسی سرور و پهنای باند مناسب و البته در خارج از کشور در دسترس باشد.

پروکسی سرور های قابل دسترس برای عموم

پروکسی های باز، سرورهایی هستند که یا به عمد یا برای ارتباط با کامپیوترهای راه دور باز گذاشته شده اند. معمولا معلوم نیست که آیا پروکسی های باز برای سرویس دهی به عموم مردم باز گذاشته شده اند یا به علت اشتباه در تنظیمات باز هستند و مردم می توانند از آنها استفاده کنند.

هشدار: با توجه به تفسیر قوانین محلی، استفاده از پروکسی های باز ممکن است دسترسی غیر قانونی تلقی شده و استفاده کنندگان از این پروکسی ها به خاطر «دسترسی غیرمجاز» مورد مجازات قرار گیرند. به همین دلیل استفاده از پروکسی سرورهای باز پیشنهاد نمی شود.

یافتن پروکسی‌های باز

بسیاری از وبسایتها لیست پروکسی‌های از راه دور را در اختیار می‌گذارند ولی هیچ تضمینی وجود ندارد که آن پروکسی هنوز هم فعال باشد. هیچ چیزی ضامن این مطلب نیست که اطلاعات این فهرست‌ها، خصوصا اطلاعات مربوط به سطوح گمنامی و موقعیت جغرافیایی پروکسی‌ها دقیق و صحیح باشد. آگاه باشید که از این پروکسی سرورها با مسوولیت خودتان استفاده می‌کنید.

وبسایت‌های حاوی فهرست پروکسی‌های باز :

<http://www.samair.ru/proxy/>
<http://www.antiproxy.com/>
<http://tools.rosinstrument.com/proxy/>
<http://www.multiproxy.org/>
<http://www.publicproxyservers.com/>

نرم افزار ProxyTools / Local Proxy :

<http://proxytools.sourceforge.net>

پروکسی‌های باز روی پورتهای غیر معمول

برخی از کشورهایی که در سطح ملی فیلترگذاری می‌کنند، دسترسی به پورتهای معمولی مورد استفاده پروکسی سرورها را نیز مسدود می‌کنند. «پورت» یا «درگاه» یک محل اتصال منطقی است که توسط پروتکل‌های خاص مورد استفاده قرار می‌گیرد. سرویس‌های اینترنتی مختلف اطلاعات را با استفاده از پورتهای مختلف مبادله می‌کنند. سازمان Internet Assigned Numbers Authority یا IANA بعضی پورتهای خاص را به بعضی پروتکل‌های خاص اختصاص می‌دهد. برای مثال، پورت 80، مسوول انتقال اطلاعات HTTP است. وقتی شما صفحه‌ای در مرورگر باز می‌کنید، در حقیقت روی پورت 80 به سرویس‌دهنده آن سایت متصل شده‌اید. پروکسی سرورها هم به شکل پیش فرض از یکسری پورت استفاده می‌کنند. به همین دلیل بسیاری از فن‌آوری‌های فیلترگذاری اجازه استفاده از این پورتهای را به افراد نمی‌دهند. در این وضعیت دور زدن موفق، وابسته به استفاده از پروکسی سرورهایی است که بر روی پورتهای غیر استاندارد کار کنند.

<http://www.web.freerk.com/proxylist.htm>

مسائل امنیتی مرتبط با پروکسی سرورها

تنظیمات پروکسی سرورها از اهمیت ویژه‌ای برخوردار است زیرا امنیت و گمنامی استفاده‌کنندگان کاملاً به آن وابسته است. علاوه بر عدم استفاده از رمزنگاری، این خطر هم وجود دارد که پروکسی سرورها اطلاعاتی در مورد کاربری که صفحه مورد نظر را درخواست کرده در اختیار جایی که صفحه از آن درخواست شده قرار دهند که این امر به نوبه خود باعث شناسایی هویت کاربر نهایی شود. علاوه بر این ممکن است ارتباطات شما به شکل متن ساده باشد و در نتیجه کسی که مشغول بررسی اطلاعات ارسالی به شبکه است به راحتی آن را شنود کند. همیشه باید در یاد داشته باشید که کل اطلاعات مبادله شده با پروکسی توسط مسوول پروکسی سرور قابل بررسی هستند.

جستجو به دنبال پروکسی‌های آزاد و استفاده از آنها هم پیشنهاد نمی‌شود. این پروکسی‌ها معمولاً به دلیل در دسترس بودن استفاده می‌شوند و با وجود کارایی آنها در دور زدن فیلترهای اینترنتی، قابلیت‌های امنیتی خوبی ندارند.

همانند پروکسی‌های تحت وب، پروکسی سرورها نیز مسائل امنیتی مشابهی دارند. برنامه‌ها و کوکی‌های مضر هنوز ممکن است به کامپیوتر کاربرنهایی وارد شوند و حتی در صورت استفاده از رمزگذاری نیز احتمال حملات MITM و بررسی اثرانگشت HTTPS باقی می‌ماند همچنین باید توجه کرد که در صورت استفاده از یک sock proxy (شکل خاصی از پروکسی که علاوه بر ترافیک وب می‌تواند اطلاعات دیگر را نیز منتقل کنند) ممکن است برخی اطلاعات حساس از مرورگر شما به بیرون درز کنند. در زمان درخواست دریافت اطلاعات از یک وبسایت، نام دومین آن به نشانی IP تبدیل می‌شود. برخی جستجوگرها این کار را به صورت محلی انجام می‌دهند و در نتیجه این فرآیند در پروکسی انجام نمی‌شود. در این موارد، نشانی IP درخواست شده توسط Domain Name Server یا DNS‌های درون کشور فیلترکننده اینترنت بررسی می‌شود.⁵

استفاده از پروکسی سرورهای باز و قابل دسترسی برای عموم، معمولاً پیشنهاد نمی‌شود و فقط باید توسط کسانی استفاده شود که در محیط‌های کم‌خطر می‌خواهند به شکل موقت و موردی از دورزننده‌ها استفاده کنند و به دنبال انتقال اطلاعات حساس نیز نیستند.

⁵ برای کسب اطلاعات بیشتر به وبسایت Tor مراجعه نمایید : <http://tor.eff.org/cvs/tor/doc/CLIENTS>

تونل زدن



تونل زدن، که به «port forwarding» هم شناخته می‌شود به افراد اجازه می‌دهد که ترافیک گیرایمن و بدون رمزگذاری را در پروتکلی رمزگذاری شده کپسوله کنند (یعنی درون آن قرارش داده و ارسالش کنند). کاربری که در محیط سانسور شده قرار دارد باید نرم‌افزاری را از شبکه بگیرد که می‌تواند تونلی به کامپیوتر درون دنیای آزاد بزند. خدمات عادی رایانه کاربر هنوز در دسترس هستند با این تفاوت که حال توسط یک تونل شفاف به کامپیوتر

آزاد منتقل شده و نتایج به آن بازگردانده می‌شوند. محصولات تونل‌زنی متفاوتی وجود دارند. کاربرانی که دارای رابطی در کشورهای بدون فیلتر هستند، می‌توانند تونل‌های شخصی خود را ایجاد کنند. در حالی که آنانی که به این رابطها دسترسی ندارند، می‌توانند با پرداخت اشتراک ماهیانه، از سرویس‌های تونل‌زنی تجاری استفاده کنند.

به هنگام استفاده از نرم‌افزارهای تونل‌زنی رایگان باید متوجه باشید که این خدمات معمولاً دارای تبلیغ هستند. درخواست نمایش این تبلیغ‌ها معمولاً به شکل متن ساده صورت می‌گیرد و در نتیجه مسوول بازرسی می‌تواند از روی آن‌ها حدس بزند که شما مشغول تونل‌زنی هستید. علاوه بر این بسیاری از نرم‌افزارهای تونل‌زنی از پروکسی‌های socks استفاده می‌کنند که ممکن است تقاضای بازگشایی اسامی دامنه از طریق طی آن‌ها به بیرون درز کند.

<http://www.http-tunnel.com/>

<http://www.hopster.com/>

<http://www.htthost.com/>

مزایا :

برنامه‌های تونل‌زنی امکان رمزگذاری ارتباطات را فراهم می‌کنند. برنامه‌های تونل‌زنی معمولاً می‌توانند پروتکل‌های بسیاری را پروکسی کنند و نه فقط ارتباط وب را. در حال حاضر سرویس‌دهنده‌های تجاری‌ای موجود هستند که کاربرانی که رابطی در خارج ندارند نیز می‌توانند از آن‌ها استفاده کنند.

معایب :

سرویس‌دهندگان تونل‌زنی تجاری، شناخته شده هستند و ممکن است در حال حاضر هم سانسور باشند. تونل‌زنی را نمی‌توان در مراکز دسترسی عمومی استفاده کرد زیرا کاربران اجازه نصب نرم افزار بر روی رایانه کتابخانه‌ها یا کافی‌نت‌ها را ندارند.

استفاده از تونل‌زنی نسبت به روش‌های دیگر عبور از فیلتر به دانش فنی بیشتری احتیاج دارد. تونل‌زدن برای کاربرانی که توانایی‌های فنی بالاتری داشته و نیاز به دورزدن فیلتر (و نه گمنامی) برای ارتباطات وب و ارتباطات دیگر خود دارند و معمولا برای اتصال به اینترنت از کامپیوترهای عمومی استفاده نمی‌کنند، مناسب است. سرویس‌های تونل‌زنی تجاری یکی از بهترین انتخاب‌ها برای افرادی است که در کشورهای فیلترگذاری شده زندگی می‌کنند و رابط قابل اعتمادی در خارج از کشور ندارند.

سیستم‌های ارتباطی گمنام

فن‌آوری‌های دورزننده و سیستم‌های ارتباطی گمنام مشابه هم و حتی گاهی بسیار مرتبط هستند ولی با دو معیار کاملا متفاوت. تمرکز سیستم ارتباط گمنام بر این است که گمنامی و خلوت استفاده کننده را با محفوظ کردن هویت وی از آرایه‌کننده‌های محتوا، تامین کند. علاوه بر این، سیستم‌های پیشرفته از انواع روش‌های مسیریابی‌ها استفاده می‌کنند تا مطمئن شوند که هویت کاربر در سیستم‌های مخابراتی نیز گمنام مانده است. سیستم‌های دورزدن الزاما روی گمنامی، تمرکز نمی‌کنند. در مقابل تمرکز آن‌ها بر این است که کاربر بتواند بر محدودیت‌های احتمالی نسبت به آنچه می‌تواند از شبکه ارسال، دریافت کند یا به آن ارسال کند غلبه کند. دور زدن محدودیت‌های اعمال شده بر محتوای اینترنت معمولا نیازمند حدی از ارتباطات ایمن و گاهی هم مخفی کردن هویت کاربر است ولی اینها الزاما به معنی گمنامی کامل فرد نیستند.

سیستم‌های ارتباطی گمنام عموما برای دورزدن فیلتر هم استفاده می‌شوند. مزیت آن‌ها این است که در حال حاضر شبکه‌های بسیاری وجود دارند که می‌توان با پیوستن به آن‌ها، برای دور زدن محدودیت‌های دسترسی به محتوا استفاده کرد و تازه اینکار را به شکل گمنام انجام داد.

استفاده از سیستم‌های ارتباطی گمنام محدود به رایانه‌هایی است که کاربر لاقط تا حدی امکان نصب برنامه بر روی آن‌ها را دارد. کسانی که از طریق رایانه‌های عمومی مانند کتبخانه‌ها یا کافی‌نت‌ها به اینترنت دسترسی دارند، عموما قادر نخواهند بود از این دورزننده‌ها استفاده کنند. همچنین این دورزننده‌ها معمولا باعث کاهش سرعت کار با اینترنت هم می‌شوند.



کاربرانی که در صدد عبور از فیلترهای اینترنتی در سطح ملی یا ISPها هستند، ممکن است با اقدامات مقامات فیلترگذاری جهت بستن سیستم‌های ارتباطی گمنام مواجه شوند. اگر سیستمی که استفاده می‌شود همیشه از طریق یک پورت ثابت کار کند، نرم افزار فیلترگذاری به آسانی می‌تواند به شکلی تنظیم شود که از دسترسی به این پورت جلوگیری کند. هر چه سیستم ارتباطی گمنام کننده شناخته شده‌تر باشند به همان نسبت خطر مسدود شدنش هم بیشتر است.

علاوه بر این، برای مبارزه با سیستم‌هایی که از آدرس‌های ارتباطی عمومی یا شناخته شده استفاده می‌کنند، مقامات فیلترگذاری به آسانی دسترسی به آن آدرسها را مسدود خواهند کرد. مقامات فیلتر گذاری ممکن است سرویس‌دهنده خاص خود را راه بیاندازند و سپس تلاش کنند هر کسی که به آن متصل می‌شود را شناسایی کنند. در برخی محیط‌های محدود شده که دسترسی به این سرویس‌ها زیر نظر قرار دارد، به کارگیری آن‌ها ممکن است توجه زیادی را به سمت استفاده کننده جلب کند.⁶

مزایا:

این سیستم‌ها هم امنیت را فراهم می‌کنند و هم گمنامی را. این سیستم‌ها عموماً قابلیت پروکسی کردن ایمن بسیاری از پروتکل‌ها، و نه فقط وب، را فراهم می‌کنند. آنها عموماً دارای اجتماعی از کاربران و توسعه دهندگان هستند که می‌توانند به افراد کمک‌های فنی ارائه دهند.

معایب:

این سیستم‌ها به طور خاص برای دور زدن فیلتر طراحی نشده‌اند، به شکل عمومی شناخته شده هستند و ممکن است به راحتی فیلتر شوند. آنها از سوی کاربرانی که از مراکز عمومی مانند کافی‌نت‌ها یا کتابخانه‌های عمومی به اینترنت دسترسی دارند قابل استفاده نیستند زیرا این افراد نمی‌توانند نرم افزارهای مورد نیاز را روی این رایانه‌ها نصب کنند.

⁶ برای کسب اطلاعات بیشتر در زمینه حملات احتمالی به سیستم های دورزننده به مقاله بنت هاسلتون مراجعه نمایید

(فهرست ضعف های احتمالی موجود در سیستم های دورزننده سانسور اینترنتی) در <http://peacefire.org/circumventor/list-of-possible-weaknesses.html> و پاسخ آن توس پل بارانوسکی در www.peekbooty.org/pbhtml/downloads/ResponseToLopwisticic.pdf

- Tor شبکه‌ای از تونل‌های مجازی است که به مردم و گروه‌ها اجازه می‌دهد ایمنی و خلوت خود در اینترنت را افزایش دهند. این برنامه همچنین به توسعه‌دهندگان نرم‌افزارها اجازه می‌دهد تا ابزارهای ارتباطی با ایمنی درون‌ساز ایجاد کنند. Tor زیربنایی برای بسیاری از نرم‌افزارها است که به سازمان‌ها و افراد اجازه می‌دهد اطلاعات را بدون نگرانی از خلوت خود بر روی شبکه‌های عمومی به اشتراک بگذارند.
<http://tor.eff.org>
- JAP امکان گشتزنی گمنام در اینترنت را فراهم می‌کند. کاربران به جای اینکه مستقیم به سایت مقصد متصل شوند چند بار به شکل رمزگذاری شده بین رابط‌های مختلف (mix) دور می‌زنند.
http://anon.inf.tu-dresden.de/index_en.html
- Freenet یک نرم‌افزار آزاد و رایگان است که به شما اجازه می‌دهد اطلاعات را بدون نگرانی از سانسور بر روی شبکه منتشر کنید یا دریافت کنید. این نرم‌افزار کاملاً غیر متمرکز بوده و ناشران و کاربران اطلاعات کاملاً گمنام هستند.
<http://freenet.sourceforge.net>

استفاده از چنین سیستم‌هایی ممکن است نیاز به مهارت‌های فنی بالایی داشته باشد. سیستم‌های ارتباطی گمنام مناسبترین روش برای کاربرانی است که قابلیت فنی بالا داشته و نیازمند دورزدن فیلتر و گمنامی برای ارتباطات مختلف شبکه‌ای هستند و از مراکز عمومی نیز به اینترنت متصل نمی‌شوند.

نتیجه‌گیری

تصمیم‌گیری برای استفاده از یکی از فن‌آوری‌های دورزننده باید بسیار جدی، پس از تحلیل و با توجه به نیازهای خاص، وجود منابع در دسترس و مسائل امنیتی کاربر نهایی گرفته شود. فن‌آوری‌های گوناگونی برای کاربرانی وجود دارد که می‌خواهند از فیلترهای اینترنتی عبور کنند. در عین حال، استفاده از آنها برای دور زدن موفق و پایدار، در گرو عوامل گوناگونی است که شامل سطح مهارت فنی کاربر، خطرات امنیتی بالقوه و ارتباطات قابل اطمینان خارج از کشور سانسور شده است. دولت‌ها نیز ممکن است برای مقابله با این مساله اقداماتی بکنند و برخی فن‌آوری‌های دور زدن را به خوبی محدود کنند.

کلید اصلی رسیدن به سیستم‌های دور زننده خوب و پایدار، اعتماد و بهره‌وری است. سیستم‌های دور زننده باید با در نظر گرفتن کاربران در شرایط خاص ایجاد و برای محیط‌های مختلف تطبیق داده شوند. آنها باید ایمن، قابل تنظیم و مخفی باشند. بین رایه کننده سیستم دور زننده فیلتر و کاربر نهایی باید اعتماد به وجود آمده و محیط خاص سیاسی و قانونی که کاربر نهایی در آن فعالیت می‌کند، درک شده و کاربر نیز از محدودیت‌های فن‌آوری‌های دور زدن مطلع باشد.

** Nart Villeneuve مدیر تحقیقات فنی در CitizenLab است که یک آزمایشگاه میان رشته‌ای واقع در مرکز مانک برای تحقیقات بین‌المللی در دانشگاه تورنتو است. به عنوان یک فرد دانشگاهی و تولیدکننده نرم‌افزار، او اخیراً بر روی (ONI) OpenNet Initiative فعالیت کرده و فیلترگذاری متون اینترنتی و دستاوردهای تحقیقاتی در سراسر جهان را بررسی می‌نماید. او همچنین به ثبت و ارزشیابی فن‌آوری‌های دورزننده موجود و همچنین ایجاد فن‌آوری‌های جدید پرداخته است. علاوه بر سانسور اینترنت، تحقیقات او هکتیویسم، سایبرتروریسم و امنیت اینترنت را نیز شامل می‌شود. Nart Villeneuve فارغ التحصیل دانشکده تحقیقات Peace and Conflict از دانشگاه تورنتو است.*

با تشکر

Bennett Haselton و Derek Bambauer ، Michelle Levesque

اطمینان از ایمنی کامل پست الکترونیکی

*نوشته لودوویس پیرات

در حال حاضر اکثر دولت‌ها امکان کنترل ایمیل‌ها را در اختیار دارند. پلیس حوزه‌های الکترونیک در کشورهای سرکوبگر از این وسیله برای شناسایی و دستگیری مخالفان استفاده می‌کند و بسیاری از کاربران اینترنت به خاطر ارسال یا حتی فوروارد یک ایمیل به زندان افتاده‌اند. یک مخالف سیاسی در مالدیو در سال 2002 به علت مکاتبه با سازمان عفو بین‌المللی به 15 سال زندان محکوم شد. یک مشترک اینترنت در سوریه نیز از فوریه سال 2003 به علت فوروارد یک خبرنامه الکترونیکی در زندان است.

بنابراین در این جا چند نکته ذکر می‌شود تا از ایمنی ایمیل خود مطمئن شوید.

استفاده از سرویس ایمیلی که توسط سرویس‌دهندگان اینترنت (ISP) همچون AOL ، Wanadoo یا Free یا هر شرکت دیگری در اختیار شما قرار می‌گیرند تضمین‌کننده ایمنی ایمیل نیستند. صاحبان شبکه‌هایی که پیام‌های شما از آنها عبور می‌کنند، می‌توانند به راحتی پیام شما را شنود کنند. هنگامی که مقامات رسمی یک کشور بخواهند مشترکین اینترنت را تحت نظارت و کنترل قرار دهند، از طریق ISP آنها اقدام کرده و ایمیل‌های موجود بر روی سرورهای آنها را می‌خوانند.

شناسه‌های ایمیل تحت وب (مانند Yahoo و Hotmail) از ایمنی بیشتری برخوردارند چرا که از هیچ سرور یا ISP محلی‌ای استفاده نمی‌کنند. برای خواندن پیام‌هایی که از طریق شناسه‌های ایمیل تحت وب ارسال می‌شوند یا باید به زور وارد سرور آنها شوید یا پیام‌های در حال انتقال را شنود کنید، کاری که از نظر فنی مشکل‌تر است. متأسفانه این شیوه حفاظت، نسبی است و متخصصان پلیس یا هکرها به راحتی می‌توانند به ایمیل‌شما وارد شده، آن را بخوانند.

رمزگذاری (نوشته‌های محافظت شده با رمز) بهترین راه برای کسب اطمینان واقعی نسبت به ایمنی پیام‌ها است که برای رسیدن به آن دو روش وجود دارد.

رمزگذاری کلاسیک

«آن» و میشل می خواهند پیام های سری مبادله کنند، پس بر روی کد و کلید رمزگذاری و رمزگشایی توافق می کنند. بعد از این پیام هایشان را با استفاده از این کدها و کلیدها مبادله می کنند.

نقص این روش این است که اگر نفر سوم پیام هایی که طی آنها میشل و «آن» مشغول مبادله کد و کلید رمزگذاری هستند را شنود کند، خواهد توانست از آنها برای بازگشایی دیگر پیام ها و حتی ارسال پیام های دروغین به میشل یا «آن» استفاده کند. پس میشل و «آن» باید کلیدها و کدها را به شکلی مبادله کنند که هیچ کس نتواند آنها را شنود کند، مثلا در یک دیدار رو در رو.

رمزنگاری نامتقارن

بهترین راه برای حل این مشکل استفاده از شیوه رمزنگاری «نامتقارن» است. برای این کار باید دو کلید داشته باشیم، یکی برای رمزگذاری و یکی برای رمزگشایی. جزئیات کلید رمزگذاری (یا «کلید عمومی») را می توان بدون نگرانی روی اینترنت ارسال کرد چرا که نمی توان از آن برای رمزگشایی پیام ها استفاده کرد. کلید رمزگشایی (یا «کلید خصوصی») هم هیچگاه نباید مبادله شود.

با شیوه رمزنگاری نامتقارن، «آن» جفت کلید مخصوص خود را دارد (یک کلید عمومی که به بقیه می دهد و یک کلید خصوصی که پیش خودش نگاه می دارد). «آن» کلید عمومی خود را برای میشل می فرستد و میشل با استفاده از آن، پیام هایی که می خواهد به «آن» بفرستد را رمزگذاری می کند. میشل هم با جفت کلید خودش همین کار را می کند؛ کلید عمومی را برای «آن» می فرستد و کلید خصوصی را برای رمزگشایی استفاده می کند. حالا «آن» و میشل می توانند در کمال امنیت، پیام هایشان را مبادله کنند.

البته از آنجایی که کلید عمومی بدون حفاظت در اینترنت منتقل می شود، بهتر است شیوه ای نیز برای آزمایش اعتبار و هویت فرستنده مشخص شود. هر کلید یک «اثر انگشت» (رشته ای کوتاه از کاراکترها) دارد که به راحتی می توان آن را در رو یا پشت تلفن مبادله کرد.

یک کلید آزمایش اعتبار نشده ممکن است یک کلید تقلبی از سوی شخص سوم با نیتی پلید باشد که رمزگذاری را بی اثر می کند. اعتبار رمزگذاری نامتقارن مطلقا وابسته به مخفی نگاه داشتن کلید خصوصی و آزمایش اعتبار کلید عمومی طرف دیگر نیست.

OpenPGP (Open Pretty Good Privacy) یک رمزگذار استاندارد نامتقارن است.

مشهورترین و بهترین نرم افزار برای ایجاد و استفاده از جفت کلیدهای نامتقارن و مدیریت کلیدهای عمومی دیگران، GnuPG (GNU Privacy Guard) است. این برنامه هم با نرم افزارهای ایمیل، مانند «تاندربرد» و «آوتلوک» کار می کند و هم با ایمیل های تحت وب و هم با برنامه های چت.

می توانید GnuPG را از طریق این پایگاه دریافت کنید:
www.gnupg.org
برای دسترسی به نسخه های خاص تحت ویندوز به اینجا مراجعه کنید:
www.winpt.org

** Ludovic Pierrat مهندس کامپیوتر گرداننده Wa است؛ شرکتی در زمینه تولیدات و مشاوره فناوری اطلاعات.*

جام جهانی سانسور اینترنت

*نوشته جولین پن

بسیاری از دولت‌های خودکامه دنیا تلاش می‌کنند تا مطالب مورد مطالعه و فعالیت‌های اینترنتی شهروندان خود را کنترل کنند. آنها روز به روز در محدود کردن و ممانعت از دسترسی به مطالب «مشکل‌دار» پیشرفت می‌کنند و عموماً نیز این کار توسط فن‌آوری‌هایی صورت می‌گیرد که از شرکت‌های آمریکایی خریداری شده است. چین در این امر بسیار پیش‌رفته و جام قهرمانی را کسب نموده است. اما رقابت در سال‌های اخیر داغ‌تر شده است. هر کدام از کشورهای این حوزه دارای روش‌ها و راهبردهای خاص خود هستند اما همه آنها یک هدف را دنبال می‌کنند و آن چیزی نیست جز سبقت از دیگران.

چین، قهرمان جهان

چین اولین دولت خودکامه‌ای بود که دریافت، بدون اینترنت هیچ کاری نمی‌تواند انجام دهد و در نتیجه لازم است آن را زیر کنترل خود بگیرد. این کشور یکی از معدود کشورهایی است که در عین گسترش تسهیلات اینترنتی، تمام انتقادات و مطالب مخالف دولت را مسدود می‌کند. راز مطلب کجا است؟ تلفیق هوشمندانه سرمایه‌گذاری، فن‌آوری و دیپلماسی.

پن ده‌ها میلیون دلار برای تجهیزات پیچیده فیلترگذاری و نظارت بر اینترنت هزینه کرده است. این سیستم مبتنی بر لیست سیاهی از وبسایت‌هایی است که همواره در حال روزآمد شدن است. دسترسی به سایت‌های «برانداز» - که آنقدر وسیع است که وقاحت‌نگاری، انتقاد سیاسی و سایت‌های طرفدار تبت یا استقلال تایوان را نیز شامل می‌شود - در سطح شاهراه‌های اینترنتی کشور مسدود شده‌اند. البته سانسور به اینجا ختم نمی‌شود و رژیم به شکل خودکار می‌تواند دسترسی به جستجوهای «مشکوک» که مثلاً حاوی جستجوی تلفیقی «تیانانن» و «فاجعه» باشند را شناسایی و دسترسی به آنها را محدود کند.

این حکومت قادر است که انجمن‌ها و تالارهای گفتگوی اینترنتی را نیز تقریباً بلافاصله سانسور کند. نرم‌افزارهای هنرمندانه و پلیس حوزه‌های مجازی که تصور می‌رود تعداد آنها باید ده‌ها هزار نفر باشد، دولت را قادر ساخته‌اند که انجمن‌های On line را که در سال‌های اخیر رشد زیادی داشته‌اند و بحث‌های سیاسی در آنها فعال بوده است را کنترل کند. به طور مثال، فراخوانی برای انتخابات آزاد در این انجمن‌ها عمری بیشتر از نیم ساعت ندارد و بلافاصله سانسور می‌شود.

وزارت صنایع و اطلاعات نیز به خوبی وبلاگ‌ها را هدف گرفته است و در قراردادی با ارایه دهندگان سرویس وبلاگ در چین، آن‌ها را مجاب کرده است که کاربران را سانسور کنند. در نتیجه نوشته‌ای درباره دالایی لاما، به هنگام دیده شدن بر روی وبلاگ، با کلی فضای خالی ظاهر می‌شود که در اصل حاوی کلمات «غیر مجاز» جایگزین شده‌اند.

اما چین چگونه به چنین تجهیزات پیشرفته‌ای دست پیدا کرده در حالی که تنها یک دهه قبل هیچ شرکت اینترنتی بزرگی در این کشور فعالیت نداشت؟ با کمک شرکت‌های بزرگ امریکایی که تحت مدیریت Cisco قرار دارند. این شرکت‌ها با هدف به دستگیری بخش کوچکی از بازار اینترنتی صد میلیونی چین، چشم خود را به روی شیوه‌ای که فن‌آوری آن‌ها در چین استفاده می‌شود بسته‌اند. حتی برخی از آنها نیز ممکن است در جهت ایجاد فیلتر و نظارت بر اینترنت با دولت ارتباط مستقیم داشته باشند.

پکن همچنین بزرگترین موتورهای جستجوی اینترنتی جهان را به زانو درآورده است. چند سال قبل Yahoo! پذیرفت که کل اطلاعاتی که از نظر چین نامناسب است را از فهرست نتایج جستجوی خود حذف کند. گوگل سال‌ها در مقابل این فشار مقاومت کرد ولی حالا به نظر می‌رسد که در جهت پذیرش آن پیش می‌رود.⁷

پلیس و دادگاه‌های این کشور نیز با نویسندگان وبسایت‌هایی که مطابق با قوانین تعیین شده از سوی دولت حزب کمونیست رفتار نمی‌کنند، برخورد بسیار خشن دارند. هفتاد و پنج نفر از مخالفان که تلاش نموده‌اند در حوزه‌های مجازی اخبار مستقل را نشر کنند، اکنون در زندان به سر می‌برند و برخی از آن‌ها نیز به بیش از 10 سال حبس محکوم شده‌اند.

بنابراین، قبل از برپایی هر وبلاگی در چین بهتر است که قوانین و مقررات حاکم در این حوزه را به درستی بررسی کنید. با توجه به این که این کشور به عنوان پیشگام سانسور اینترنتی در سراسر جهان شناخته شده است و وبلاگ نویسانی که در این کشور به سر می‌برند، باید بسیار مراقب بوده و هوشمندانه عمل کنند.

ویتنام : تیمی بسیار خشن

ویتنام به الگوی چین وفادار مانده و از آن پیروی می‌کند اما با توجه به این که آنها از نظر ایدئولوژیک دیدگاه‌های سخت‌تری دارند، قابلیت‌های اقتصادی و فن‌آوری همسایه خود را به دست نیآورده‌اند. این کشور دارای پلیس اینترنتی‌ای است که موارد «براندازی» را در سایت‌ها مسدود می‌کند و مراقب کافی‌نت‌ها است. البته پلیس با مخالفان فعال در حوزه مجازی هم برخوردهای خشنی داشته است. در حال حاضر سه نفر از کسانی که جرات کرده‌اند در اینترنت از دموکراسی صحبت و از آن دفاع کنند، بیش از سه سال است که در زندان هستند.

⁷ گوگل در سال 2006 تسلیم فشارهای دولت چین شد و نسخه سانسور شده google.cn را راه‌اندازی کرد که مطابق میل دولت چین سانسور شده است.

تونس : بازیگران الگو



رئیس جمهور زین العابدین بن علی که خانواده اش انحصار اینترنت در تونس را در دست دارند، توانسته سیستم بسیار موثری برای سانسور اینترنت ایجاد کند. دسترسی به همه وبسایت‌های مخالف ممنوع بوده و مشترکین حتی قادر به دیدن چند پایگاه خبری معدود مانند روزنامه لیبراسیون فرانسه نیز نیستند. همچنین دولت تلاش می‌کند تا مردم را از استفاده از ایمیل‌های تحت وب بازدارد چرا که کنترل آن نسبت به ایمیل‌های استانداردی مانند آوتلوک سخت‌تر است. ورود به صندوق ایمیل Yahoo! در یک کافی‌نت تونسی ممکن است بیست دقیقه طول بکشد و این احتمال هم وجود دارد که در نهایت پیام Time out یا Page not found پدیدار شود. وبسایت گزارشگران بدون مرز نیز از داخل کشور قابل دسترسی نیست.

ولی به نظر می‌رسد که جامعه بین‌المللی به این نتیجه رسیده که عملکرد تونس در سطح محلی قابل قبول است زیرا اتحادیه ارتباطات خبراتی بین‌المللی وابسته به سازمان ملل متحد (ITU) این کشور را برای میزبانی اجلاس جهانی جامعه اطلاعاتی (WSIS) در نوامبر 2005 انتخاب نمود. این ایده که تونس الگوی توسعه اینترنتی به شمار می‌رود بسیار ناراحت‌کننده است.

ایران : جوخه مرگ

سانسور اینترنتی در آسیا تنها از سوی رژیم‌های کمونیست اعمال نمی‌شود. سیستم فیلترگذاری در ایران طی سال‌های اخیر بسیار پیشرفت کرده و وزارت اطلاعات [منظور وزارت اطلاعات و فناوری اطلاعات (وزارت پست و تلگراف و تلفن سابق)] ادعا می‌کند که اخیراً راه دسترسی به صدها هزار وبسایت را مسدود کرده است. ملاحظاتی این کشور تمام مضامینی که به نوعی به مسائل جنسی ارتباط پیدا می‌کنند را ممنوع کرده‌اند و بعلاوه قادر به تحمل حضور پایگاه‌های خبری مستقل نیز نیستند.

دولت این کشور قادر به اعمال بدترین گونه سانسور بوده و با زندانی کردن بیست وبلاگ‌نویس طی ده ماه، مقام اول را در سال 2005 کسب نموده است. در اول آگوست 2005 هنوز سه نفر از آنان در زندان هستند.

کوبا : «افسانه»

دولت کوبا به دلیل مهارتش در کنترل مکالمات تلفنی مشهور است اما قابلیت آنها در سانسور اینترنت نیز شایان ذکر است. الگوی چینی‌ها مبنی بر تشویق فعالیت‌های اینترنتی در عین کنترل آن بسیار گران است، بنابراین رئیس‌جمهور فیدل کاسترو راه آسانتری را انتخاب کرده - جلوگیری از دسترسی اکثریت مردم به اینترنت.



دسترسی به اینترنت در کوبا مزیتی است که تنها تعداد معدودی از آن برخوردار بوده و برای استفاده از آن باید از حزب کمونیست اجازه بگیرند. البته حتی زمانی که به صورت غیرقانونی موفق شوید به اینترنت دست پیدا کنید نیز می بینید که تنها نسخه سانسور شده آن در دسترس است.

تعداد بسیار کمی از مردم می دانند که کوبا یکی از کشورهایی است که کمترین دسترسی به اینترنت در آن وجود دارد و در آن متون موجود بر روی اینترنت هم مانند رسانه های سنتی شدیداً کنترل می شوند. چرا مردم از این موضوع خبر ندارند؟ احتمالاً پاسخ این سوال، افسانه قدرت همیشگی انقلاب کوبا است.

عربستان سعودی : اهداف مشخص

مقامات عربستان سعودی آشکارا می پذیرند که اینترنت در کشور آنها سانسور است. البته در آنجا، مانند چین با Page not found مواجه نمی شوید بلکه به صفحه ای می روید که می گوید این صفحه توسط فیلترهای دولت مسدود شده است. واحد خدمات اینترنتی (ISU) با افتخار اعلام می کند که دسترسی به چهارصد هزار سایت را محدود نموده و فرمی On line نیز تهیه کرده است که کاربران می توانند از طریق آن، سایت های جدیدی که فکر می کنند باید سانسور شوند را پیشنهاد کنند. واحد خدمات اینترنتی می گوید که هدف از بستن این وبسایت ها حمایت شهروندان علیه مضامین توهین آمیزی است که اصول اسلامی و هنجارهای اجتماعی را نقض می کنند. جالب است که یک شرکت آمریکایی به نام Secure Computing سیستم فیلترگذاری اینترنتی خود را به این کشور فروخته است.



ازبکستان: ادعا های دروغین متخصصان

وزیر اطلاعات ازبکستان در ژوئن 2005 اعلام کرد که «راهی برای سانسور اینترنت در این کشور وجود ندارد». این حرف عجیب در حالی است که دسترسی به وبسایت های مخالف در این کشور امکان پذیر نبوده و خبرنگاران اینترنتی همواره مورد تهدید و تهاجم فیزیکی قرار می گیرند .

***Jullien Pain**، رئیس بخش آزادی اینترنتی در سازمان گزارشگران بدون مرز است.

راهنمای

وبلاگ نویسان

برای

مقابله با سانسور وبلاگ‌ها در برخی افراد شور و هیجان برانگیخته و در برخی دیگر اضطراب و نگرانی را سبب شده است. برخی از مردم نسبت به وبلاگ‌ها بی‌اعتماد هستند. برخی دیگر وبلاگ‌ها را پیشگامان انقلاب جدید اطلاعاتی می‌دانند. اما وبلاگ‌نویسی ابزاری محکم و قدرتمند در دست میلیون‌ها فرد عادی است که به آزادی بیان اهمیت می‌دهند. مصرف‌کنندگان غیر فعال اطلاعات، اکنون مشتریان پر و پاقرص این شیوه جدید روزنامه‌نگاری هستند. در کشورهایی که رسانه‌های جمعی رایج تحت سانسور یا فشار قرار دارند، وبلاگ‌نویسان تنها روزنامه‌نگاران واقعی به شمار می‌روند. تنها آنها می‌توانند اخبار مستقل را در اختیار مردم قرار دهند که با این کار خطر ناخشنودی دولت و گناه بازداشت را به جان می‌خرند.

این کتاب راهنما برخی نکات فنی را در مورد نحوه راه اندازی یک وبلاگ خوب ارائه می‌دهد. اما داشتن و حفظ یک وبلاگ موفق کار بسیار دشواری است. برای سربرآوردن در میان جمع، باید اصیل بوده و اخبار و عقایدی را منتشر نمایید که از سوی رسانه‌های جمعی رایج نادیده گرفته شده‌اند. در برخی کشورها، تنها نگرانی وبلاگ‌نویسان این است که بتوانند از زندان‌های یابند. در برخی دیگر، چالش اصلی کسب اعتبار و تبدیل شدن به منبع قابل استناد اطلاعاتی است. همه وبلاگ‌نویسان با مشکلات یکسان رو به رو نیستند اما به طور کلی در خط مقدم مبارزه برای دستیابی به آزادی بیان قرار دارند.



گزارشگران بدون مرز

REPORTERS WITHOUT BORDERS

International Secretariat

5, rue Geoffroy-Marie, 75009 Paris, France

Tel: 33 1 4483-8484

Fax: 33 1 4523-1151

Website: www.rsf.org

Communication: Anne Martinez-Saiz / communication@rsf.org

Graphic design and extra illustrations: Nuit de Chine

ndf@nuitdechine.com

ISBN: 2-915536-36-8

Copyright: Reporters Without Borders 2005

Printed August 2005, France.

WITH THE SUPPORT
FROM
THE FRENCH FOREIGN MINISTRY
AND THE
FRENCH CAISSE DES DEPOTS ET CONSIGNATIONS

www.rsf.org