راهنمای
وبلاگ نویسان
برای
مقابله با سانسور

گزارشگران بدون مرز

reporters without borders

www.rsf.org

راهنمای وبلاگ نویسان
برای مقابله با سانسور

فهرست مطالب

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 هاوکسانی 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 مجله 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 کاه 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 گیلمور 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 مراجه 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 خطر نا 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 مهارتهای 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 کودک 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 وحفظ 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 گزاشگران 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 .
- عموما توسط یک نفر طراحی و اداره می شود که گاه گمنام باقی می ماند .

متون درج شده در یک وبلاگ :

- معمولا متن ساده (شامل برخی لینک های خارجی) ، گاه متن و عکس و جدیدا 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 استانداردی 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 هاي نامربوط / اسپمی که از طریق پست الکترونیك ارسال مي شوند ، وبلاگ ها نیز از سوي مزاحمان تحت هجوم گسترده پیام هاي دروغین قرار مي گیرند . این یك مشكل جدي بوده و وبلاگ نویسان و پایگاه هاي وبلاگ نویسي باید ابزار لازم براي حذف برخي از مشتركان یا پرهیز از ورود برخي آدرس ها به حوزه وبلاگ را در اختیار داشته باشند .

سندیکای محتوا (Content Syndication)
بیانگر این مطلب است که چگونه نویسنده یا مدیر یك وبلاگ، بخشي از مطالب خود را براي انتقال و نشر در پایگاه هاي الکترونیکي دیگر آماده مي سازد .

موبلاگ
اختصاري که به جاي عبارت وبلاگ هاي سیار استفاده مي شود . این عبارت به وبلاگ هایي اشاره مي کند که مي توان آنها را از دور و از هر جایي با استفاده از تلفن یا ابزار هاي دیجیتالي روزآمد نمود .

لینک پایدار / پرمالینک
پرمالینک اسم اختصار عبارت لینک پایدار است و نشاني اینترنتی هر بخشی که بر روي یك وبلاگ منتشر شده است. این کار شیوه ي مناسب و پایداري براي ارائه نشاني هر مطلب حتي بعد از بایگاني آن در وبلاگ اصلي است.

وبلاگ هاي تصویري / فوتوبلاگ
وبلاگ هایي که بیشتر شامل عکس هایي هستند که بطور مداوم به صورت زمانبندي شده روي وبلاگ قرار مي گیرند.

PODCASTING
تلفیقي از دو کلمه ي iPod و Broadcasting است که به معناي قرار دادن مطالب شنیداری و دیداری روي وبلاگ و روش هاي آسان براي قرار دادن اطلاعات روی پایگاه هاي الکترونیکي 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 معمولا بسیار کوتاه بوده و داراي پیوندهاي خارجي است و بازدید کنندگان مي توانند درباره آن نظرات خود را بیان کنند.

RSS (Really Simple Syndication)

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 خبر 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 آنلاينی كه به وبلاگ نويسان امكان مي دهد RSSهای 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

فايلي 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 خبر مي دهد.

دنبالک / Trackback

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

دفتر خاطرات وبی / Web Diary

به معناي وبلاگ است .

WIKI

نام اين پايگاه الكترونيكي از يك كلمه در زبان هاوايي " wikiwiki " (به معناي 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

Cyril Fievet و Mark – Olivier Peyer*

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 :

- آدرسي که براي دسترسی عمومی تدوین و اعلام مي 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 پلاتفورم های متنوع) دارای رنگ ها ، فونت‌ها 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 زیرباشند : http://www.thecommunity.com/myblig ، http://myblog.thecommunity.com یا http://www.thecommunity.com/mynumber

ویژگی های ارایه 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 سکوهای بین المللی

Blogger – http://www.blogger.com

رایگان

در 1999 راه‌اندازی 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 گزینه‌های چندانی در اختیار شما نمی‌گذارد.

LiveJournal – http://www.livejournal.com

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

MSN Spaces – http://www.msnspaces.com
رایگان
سکوی Microsoft که در اواخر 2004 راه‌اندازی شد. قابلیت‌های بسیاری دارد که گاهی از وبلاگ هم بیشتر است از جمله به اشتراک گذاشتن تصاویر و پیوند به Messanger . برای ثبت وبلاگ در این سیستم باید بیش از 13 سال سن داشته باشید.

سکوهای فارسی[1]
توجه کنید که امکان فیلتر شدن اطلاعات وبلاگ شما یا دست یافتن حکومت به شما در صورتی که از سکوهای فارسی استفاده کنید بسیار بیشتر است چرا که این سکوها بیشتر در ایران کار می‌کنند و الزاما 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.

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

بلاگفا – http://www.blogfa.com
سیستم نسبتا 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 اجبارا تابع قوانین کشور است.

[1] در متن اصلی سکوهای فرانسوی معرفی شده بودند ولی به دلیل کاربرد بیشتر سکوهای فارسی برای ایرانیان، در ترجمه به جای آن سکوهای فارسی معرفی شده اند.

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 پلاتفورم 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. هنگامي كه يك RSS feed را منتشر مي كنيد ، اين ابزار سر فصل هاي مطالب درج شده در وبلاگ را روي بخش خبري (برنامه هاي پست الكترونيكي مانند Outlook يا Thunderbird) قرار داده يا آن را مستقيما وارد پايگاه الكترونيكي يا وبلاگ شخصي شما مي كند . هنگامي كه وبلاگ روزآمد مي شود، RSS feed هم به همراه آن روزآمد شده و در نتيجه اطلاعات به صورت خودكار و با سرعت انتشار مي يابند .

يكي ديگر از نكات فنی وبلاگ نويسي،دنبالك است كه نشان مي دهد منشا اصلي مطالب درج شده در وبلاگ از كجا بوده و از سوي اكثر پلاتفورم ها مورد استفاده قرار مي گيرد .

هنگامي كه مطلبي مبتني و يا برگرفته از يك وبلاگ ديگر باشد مي توان امكان دنبالك را به آن اضافه كرد تا به صورت خودكار تمام پايگاه هايي كه اين مطلب را باز توليد نموده يا در مورد آن پيشنهاداتي داشته اند،مشخص شوند. ممكن است اين فرايند به نظر بسيار پيچيده باشد اما اجرای عملی آن بسيار ساده است و نتيجه رضايت بخشی هم دارد زيرا همواره دانستن اين كه ديگران نيز از

مطالب شما استفاده کرده و آن را در جايي عنوان کرده اند،لذت بخش است. همچنين اين کار برای اشاعه هر چه گسترده تر مطالب و ايجاد آگاهي بيشتر نسبت به آنها و بسط و گسترش مباحث بين وبلاگ ها بسيار مفيد است.

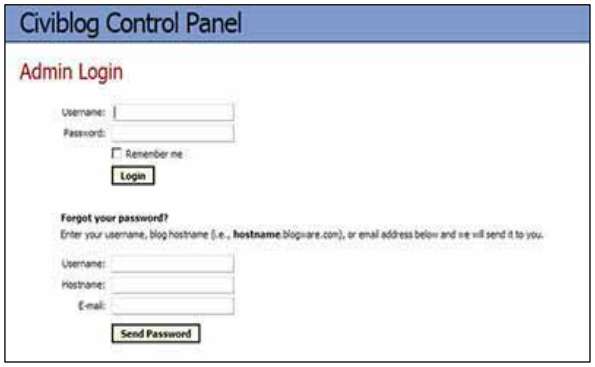
بنابراين هنگامي که قصد داريد وبلاگ خودتان را تهيه کنيد کمی برای يادگيری اين تکنولوژی وقت صرف کنيد.

صفحه اصلي CIVIBLOG

RSS feed سمت راست قرار گرفته و هرگاه يکي از اعضای گروه مطلب جديدي را درج کند، بطور خودکار روزآمد مي گردد.

ثبت نام

قبل از برپايي يك وبلاگ ابتدا بايد ثبت نام كنيد. بسياري از پايگاه هاي وبلاگ نويسي اين كار را براي مشتركين آسان نموده اند. براي ثبت نام در civiblog تنها اطلاعات ساده و اوليه مورد نياز هستند اما پايگاه بايد اطمينان حاصل نمايد وبلاگي كه ميزباني آن را پذيرفته است واقعا متعلق به گروه هاي جامعه مدني بوده و يك وبلاگ شخصي براي افراد فاميل يا دوستان نيست . از زمان ثبت نام تا نمايان شدن On line وبلاگ تنها بيست و چهار ساعت وقت لازم است تا رمزهاي مورد نياز براي دسترسي و ايجاد وبلاگ از طريق پست الكترونيك براي وبلاگ نويس ارسال شوند .



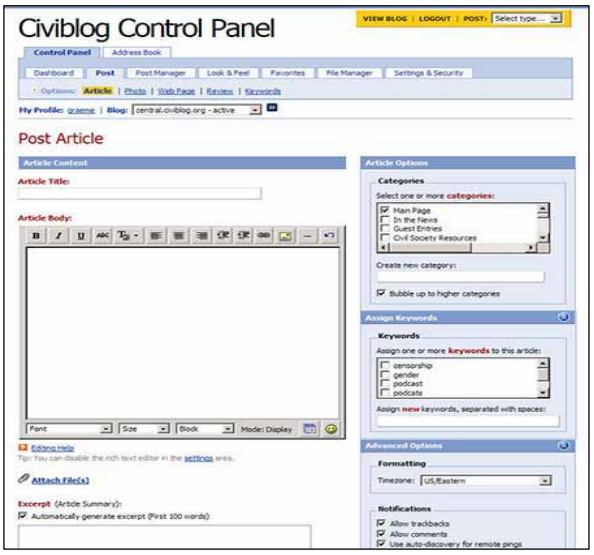
ورود به بخش مديريت

وبلاگ داراي يك « جلوی صحنه»(صفحه اي كه بازديد كنندگان آن را می بينند) و يك صفحه «پشت صحنه» است كه شما با استفاده از نام كاربري و رمز ورودي كه در زمان ثبت نام انتخاب مي كنيد مي توانيد براي روزآمد كردن و نظارت و راهبری وبلاگ خود به آن وارد شويد.

داشبورد

اكثر وبلاگ ها داراي يك صفحه داشبورد هستند يعنی صفحه ای كه در يک نگاه،مدير می تواند پی ببرد چه چيزی در وبلاگش در حال رخ دادن است؛از جمله آخرين ارسال‌ها، آخرين نظرات و آخرين دنبالک‌ها. شما می توانيد از اين صفحه به تمام تنظيمات وبلاگ دسترسي داشته باشيد، از جمله ظاهر آن،پهنای باند مصرفی،ويرايش نوشته هاي قديمي و تنظيم مجوزهای كاربران از جمله مجوز ارسال نظرات.

نحوه درج مطالب



بزرگترين تفاوت موجود بين وبلاگ ها و صفحات عادي سايت های ديگر اين است كه روزآمد نمودن وبلاگ ها بسيار آسان است. اكثر سكوها به شما اين امكان را می دهند كه در يك صفحه ساده مطالب خود را درج كنيد بدون آنكه نگران صفحه بندی اش باشيد.در پايگاه هاي جديدي چون civiblo می توانيد شكل حروف،اندازه و رنگ آن را تغيير داده و پيوندها و عكس هايي را وارد كنيد.

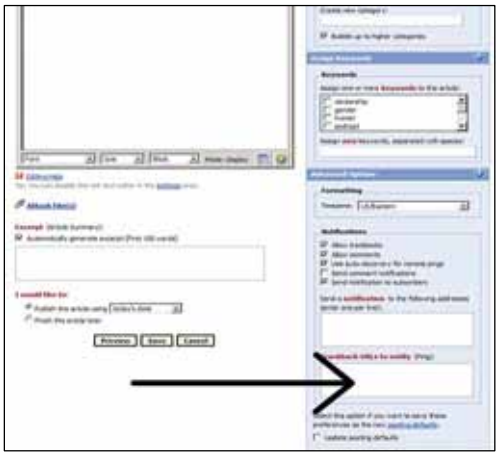
روش كار به شرح زير است :

1 . ورود به سيستم (Log in)
2 . كليک بر روي گزينه Post
3. در نظر گرفتن تيتری برای پيام مورد نظر و تايپ مطالب آن
4. صفحه بندی اطلاعات (Formatting) با استفاده از رابط های كاربری
5. گروه بندي مطلب (براي اينكه مطلب شما در كنار مطالب مشابه قرار گيرد) يا ايجاد يك گروه جديد

6. كليك روي گزينه ذخيره (Save) كه در پايين صفحه قرار گرفته است .

به همين سادگي.با كسب كمي تجربه مي توانيد از ويژگي هاي ديگري چون دنبالك،پينگ و كلمات كليدي استفاده كنيد .

دنبالك يا Trackback



افزودن يك دنبالك به مطلب نشر شده بسيار آسان است.شما بايد نام URL مطلب مورد نظر را در جعبه سمت راست صفحه كه با عنوان Trackback URLs to notify مشخص شده است وارد كنيد.حالا وقتي كه مطلب خود را ذخيره كنيد به صورت خودكار اين دنبالك نيز ايجاد مي شود.

سنديكاى RSS (RSS Syndicate)

نشر RSS سايت‌هاى ديگر نيز بسيار آسان است:

۱. وارد صفحه «پشت صحنه» وبلاگ شويد
۲. روي گزينه Favourites كليك كنيد
۳. روي گزينه RSS Headline Components كليك كنيد
٤. مطابق دستورالعمل پيش رفته و URL (كه به .xml، .rdf يا گاهي به .py يا .php ختم مي شوند RSS feed كه مي خواهيد منتشر كنيد را وارد نماييد .

۵.اسمی برای feed مورد نظر انتخاب کرده و گزینه Add feed را کلیک کنید
٦.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.روي گزينه RSS کليک کنيد : feed شما (همان اسمي است که در مرحله 5 به آن داده ايد) را وارد ستوني کنيد که مي خواهيد در آن نمايش داده شود
۱۰.روي گزينه ذخيره (Save) که پايين صفحه قرار گرفته کليک کنيد

در زير نام برخي از پايگاه هاي الکترونيکي آمده است که ريزه‌کاری‌هاي وبلاگ نويسي را توضيح مي 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/%7Ezuiker/blogging101/index.htm

وبلاگ نویسان چه موارد اخلاقی را باید رعایت کنند ؟

نوشته دن گیلمور*

همه وبلاگ نويسان به خبر نگاري علاقه ندارند. در اصل اكثر آنها خبرنگار نيستند. اما در صورت تمايل به چنين كاري بايد اصول اخلاقي را رعايت كنند.

آيا اين سخن بدان معناست كه بايد اصول اخلاقي خاصي را پذيرفته و امضا كنند ؟ الزاما خير .

كلمه حرفه ايي كه براي اطلاق به آيين هاي اخلاقي در روزنامه نگاري از آن استفاده مي كنند awash (مماس با لبه آب) است. برخي از اين آيين هاي رفتاري از قانون اساسي ايالات متحده نيز طولانی ترند زيرا در آن ها تلاش شده است تا هر مورد احتمالي پيش بيني شده و در نظر گرفته شود. برخي ديگر نيز كوتاه و مختصر بوده و تنها اصول راهنماي ساده ای را ارائه مي دهند.پايگاه الكترونيكي خبرنگاري در حوزه مجازي (سايبرژورناليسم) با استفاده از جمعيت خبرنگاران حرفه اي كه يك گروه آمريكايي است،آيين رفتاري را براي وبلاگ نويسان تهيه نموده است(http://www.cyberjournalist.net/news/000215.php). اين حركت كاري منسجم و ارزشمند است.

تدوين آيين نامه هاي رفتاري تنها براي رسيدن به يك هدف صورت مي گيرد : القای اعتماد. اگر خواننده،بيننده و يا شنونده به گزارشي كه در پيش رو دارد ، اعتماد نداشته باشد، خواندن آن در وهله اول هيچ ارزشي نخواهد داشت. البته بدون شك استثنا هم وجود دارد كه عبارت است از مطالعه موارد غير اخلاقي براي درك كردن اصول صحيح و همچنين رسيدن به دانش درست.مصداق ضرب المثل قديمی ايرانی است كه می گويد:ادب از كه آموختي؟ از بي ادبان.

به نظر من همه اصول اخلاقي تنها در مورد يك مطلب بسيار ساده سخن مي گويند: شرافت. هرچند كه اين كلمه، حوزه بسيار گسترده اي را در بر مي گيرد اما به هرحال اگر شرافتمندانه برخورد نكنيم، نمي توانيم انتظار داشته باشيم كه مردم نيز به ما اعتماد كنند.

در نظام روزنامه نگاري آمريكايي،اعتماد با مقوله اي همراه است كه ما آن را بي طرفي مي ناميم به اين معنا كه هدف از نوشتن يك مقاله ارائه ديدگاه های مختلف درباره يک موضوع و دادن اين فرصت به خواننده است تا خود در اين باره تصميم بگيرد.

من عقيده دارم كه بي طرفي، يك هدف ارزشمند و دست نيافتني است زيرا همه ما در همه امور غرض ورزي هاي خاص خود را داريم .

در جهان خبرنگاري نوين كه از ارائه سخنراني به سوي مذاكره حركت مي كنيم، روزنامه نگاري اخلاقي كمتر مبتني بر اصول و قواعد اخلاقي بوده و بيشتر بر پايه ارزش ها و اصولي استوار است كه بنيان روزنامه نگاري شرافتمندانه را تشكيل مي دهند.

روزنامه نگاري مطلوب بر ستون هايي استوار است كه عبارتند از : دقت ، صحت ، عدالت ، شفافيت و استقلال .

مرزهای جدا کننده این مفاهیم چندان واضح نیستند. همه آن ها مستعد تفاسیر گوناگونند و حاوی ظرایف بسیار.اما من فكر مي كنم كه همه آنها، براي روي آوردن به روزنامه نگاري شرافتمندانه موثر بوده و در روزنامه نگاری On line دستيابي به آنها امكان پذير تر به نظر مي رسد. اكنون هر كدام را بررسي مي كنيم .

دقت

از هنگامي كه گزارشگر بودم تا بعدها كه ستوني در روزنامه در اختيار داشتم همواره هدفم اين بود كه هر چه بيشتر بياموزم. به هر حال جمع آوري واقعيات و آرا، پايه و اساس خبرنگاري را تشكيل مي دهند.هرگاه احساس مي كردم 95 درصد از چيزي را كه آموخته ام در متن نهایی جایی ندارد، لذت مي بردم. بهترين گزارشگراني را كه مي شناسم همواره تلاش مي كنند تا با يك فرد ديگر هم صحبت كرده و اطلاعات را از ديدگاه يك منبع ديگر نيز كنترل كنند . (آخرين سوالي كه هميشه در همه مصاحبه ها مي پرسيدم اين بود : در اين رابطه با چه كس ديگري مي توانم صحبت كنم ؟)

امروزه، «دقت» فراتر از پرسيدن سوال از كساني است كه نام و نشاني آنها در دفترچه راهنماي واقعي يا مجازي ما قرار دارد . بلكه به اين معناست كه در هر زمان ممكن از خوانندگان خود بخواهيم، داده هاي خود را ارائه كنند. يعني همان كاري را كه من در زمان نوشتن كتاب خودم درباره خبرنگاري گروه هاي مردمي در سال 2004 كردم (كه بسياري از نويسندگان نيز اكنون تلاش مي كنند براي نوشتن كتاب هاي خود از اين روش استفاده مي كنند .) فشارهاي رقابتي سبب مي شوند كه افراد كمتر به اين موضوع توجه كنند اما من ايمان دارم كه از اين به بعد خبرنگاران بيشتر از اين روش استفاده خواهند كرد .

صحت

همواره به واقعيات و مستندات تكيه كنيد.
سعي نكنيد كه تنها در مورد چيزهايي كه مي دانيد صحبت كنيد بلكه به چيزهايي كه از آن اطلاعي نداريد هم اشاره كنيد.(اگر به خواننده / شنونده / بيننده در مورد آنچه نمي دانيد اطلاع دهيد ، از او دعوت كرده ايد تا خلا هاي اطلاعاتي شما را پر كند.)
صحت به معناي تصحيح مسائلي است كه درباره آن ها اشتباه كرده ايد و همچنين اعلام اين اشتباهات. انجام اين كار به شيوه On line بسيار آسان تر است زيرا در اين شرايط مي توانيم زيان اشتباهات خود را در مورد خوانندگان جديد از بين برده يا حداقل كاهش دهيم.

عدالت

در عمل به همان اندازه كه داشتن صراحت آسان به نظر می رسد،حفظ عدالت بسيار دشوار است. ما هميشه به چشم خودمان عادل به نظر می رسيم ولی در اينجا هم می توان چند قاعده جهانی را اعمال كرد.
عدالت،داراي مفاهيم مختلفي بوده و مفهومي كه در اينجا مد نظر است، شنيدن ديدگاه ها و نقطه نظرات ديگران و تلفيق آن در روزنامه نگاري است . البته اين به معناي پذيرش و تقليد از دروغ ها يا تحريف هايی نيست كه بعضی خبرنگاران حتی در صورت مشاهده قوت يک جنبه مساله به ديگر جنبه ها، به آن ها پناه می برند.
همچنين عدالت به معناي دادن فرصت به ديگران است كه اگر تصور مي كنند، شما دچار اشتباه شده ايد نظر خود را بيان كنند. حتي اگر شما با نظر آنها موافق نباشيد. مجددا تاكيد مي كنم كه اين كار به شيوه On line بسيار آسان تر از نشريات چاپي و برنامه هاي ديداری و شنيداری است .
در نهايت مي توان گفت كه عدالت حاصل يک وضعيت ذهني است . همواره بايد بدانيم كه چه عواملي ما را پيش مي برند و هميشه ظرفيت لازم براي شنيدن سخنان مخالفان خود را داشته باشيم . اولين قانون برقراري يك گفت و گو، شنيدن است.اطمينان دارم از كساني كه فكر مي كنند من اشتباه مي كنم بيشتر ياد می گيرم تا از كسانی كه با من موافق هستند.

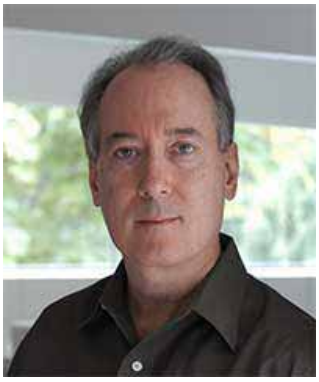
شفافيت

امروزه روشنگری به عنوان بخشي از روزنامه نگاري پذيرفته شده است . البته هميشه سخن گفتن آسان تر از عمل كردن است .

حتي به ظاهر هم نمي توان با اين عقيده مخالفت كرد كه روزنامه نگاران بايد برخي موارد خاص مانند اختلاف نظرهاي منازعه آميز مالي را آشكار سازند. اما حد و مرز اين كار تا كجا بايد باشد ؟ آيا مي توان از همه خبرنگاراني كه در حوزه هاي مختلف كار مي كنند انتظار داشت كه سفره دل خود را براي همگان باز كنند ؟ اين كار تا چه حدي منطقي و درست است ؟
تعصبات شخصي حتي تعصباتي كه آگاهي نسبت به آنها وجود ندارد بر روي فرايند روزنامه نگاري نيز تاثير مي گذارند. من يك آمريكايي هستم و با عقايد خاصي بزرگ شده ام كه ممكن است مردمان سرزمين هاي ديگر (يا حتي برخي از افراد در ايالات متحده) صراحتا آنها را نپذيرند. هر كسي بايد از چيزهايي كه بدون چون و چرا مي پذيرد آگاه بوده و در روند كار، هر از گاهي آنها را مورد بازبيني قرار دهد .
يكي ديگر از راه های شفاف عمل كردن، شيوه بيان داستان است. بايد در حد امكان به منابع استناد كرده و مضامينی كه در اختيار مردم قرار مي دهيم را با استناد به واقعيات و اطلاعات درست استحكام بخشيم.**(شايد اين كار بخشي از دقت و صراحت باشد اما به نظر مي رسد كه در اين بخش بهتر جاي مي گيرد.)**

استقلال

روزنامه نگاري شرافتمندانه به معني دنبال كردن موضوع در مسيری است كه پيش مي رود. هنگامي كه رسانه هاي جمعي ادغام شده و تبديل به چند شركت بزرگ مي شوند يا تحت كنترل دولت قرار می گيرند، اين موضوع اتفاق نمي افتد . مستقل بودن در روش On line بسيار آسان است. به راحتي مي توانيد يك وبلاگ به وجود آوريد. اما هيچ كس نيست كه بپذيرد، شركتهای تجاري و دولت روي وبلاگ نويساني كه تلاش مي كنند با استفاده از شيوه كاري جديد خود امرار معاش كنند، فشاري اعمال نخواهند كرد .
جف جارويس ،يكي از وبلاگ نويسان برجسته آمريكايي (buzzmachine.com) برخي ايده آل هاي ديگر را نيز اضافه مي كند. وبلاگ نويسان بايد به اصول اخلاقي محاوره ارج بگذارند. او به چيزی اشاره می كند كه برای من از اهميت زيادی برخوردار است و آن اين است كه: محاوره به درك متقابل مي انجامد .
در محاوره، اولين قانون گوش دادن است . اصول اخلاقي به گوش كردن بستگي دارد زيرا به اين ترتيب است كه ما مي آموزيم .



Dan Gillmore: بنيانگزارشركت رسانه هاي مردمي است كه هدف آن تقويت روزنامه نگاري مردمي و گسترش دسترسي آن است.اولين پايگاه الكترونيكي او **Bayosphere.com** واقع در بي اريا در سانفرانسيسكو است . او نويسنده كتاب «ما به عنوان رسانه ها» نيز هست:روزنامه نگاري مردمي توسط مردم و براي مردم (چاپ اوريل، 2004) .

وبلاگ او :
http://bayosphere.com/blog/danqillmore

اضافه شدن وبلاگ شما به موتورهای جستجو

نوشته اولیوراندریو*

وبلاگ ها، خودشان وب سایت هستند بنابراین توسط موتورهاي جستجويي چون google ، yahoo و MSN شناخته مي شوند. بنابراين طراحي پايگاه الكترونيكي از همان ابتدا بايد به گونه اي باشد كه به اين معيارهاي دسته بندي مكانيكي موتورها پاسخ دهد.

وبلاگ ها چند ويژگي دروني دارند كه در صورت فهرست بندي درست و جاي گرفتن در صفحات نتايج از سوي موتورهاي جستجوگر انتخاب مي شوند .

- با توجه به اين كه اين وبلاگ ها معمولا در ابتدا به صورت مجموع خاطرات شخصي هستند ، متون زيادي در آن درج مي شود كه احتمال انتخاب آنها را افزايش مي دهد . موتورهاي جستجوگر بطور معمول پايگاه هايي را كه داراي طراحي گرافيكي يا تصاوير متحرك ساخته شده با نرم افزار Flash بوده و متن نوشته شده چنداني ندارند را انتخاب نمي كنند .
- هر «مطلب» كه عموما يك صفحه را اشغال كند، از طريق پيوندي دائمي قابل دسترسي باشد و به بحث در مورد يك موضوع بپردازد، احتمال انتخاب شدن بيشتری نصبت به صفحاتی دارد كه طولاني ترند و مباحث مختلفي در آن مطرح شده است(مانند بايگاني ها و يا صفحات اصلي وبلاگ ها) .
- عنوان يك نشريه عموما در صفحه عناوين يا URL (نشاني) باز توليد مي شود. بطور مثال در وبلاگ راديو نپال آزاد به نشاني http://freenepal.blogspot.com ، هر مطلب صفحه مخصوص به خود را دارد مانند http://freenepal.blogspot.com/2005/04/state-vandalism-in-nepal.html:

عناوين اين مطلب (state vandalism in Nepal)، (ويرانگري دولت در نپال) نه تنها در صفحه URL بلكه در صفحه مربوط به متن نيز آمده است . همانطور كه در پايين نمايش داده مي شود.

بنابراين عنوان مطلب بعد از نام وبلاگ قرار مي گيرد در حالي كه در صفحه اصلي وبلاگ به تنهايي نمايان مي شود .
(http://freenepal.blogspot.com)
وجود عبارات توصيفي كليدي در عناوين صفحات (بخش مربوط به عنوان <TITLE> در زبان HTML) و در URL هاي اين اسناد معيار اصلي انتخاب توسط موتورهاي جستجوگر هستند بنابراين نكته مهم اين است كه عنوان نشريات را طوري انتخاب كنيم كه از سوي موتورهاي جستجوگر برگزيده شوند .

- پيوندها هم مانند متون به صورت خودكار به وجود مي آيند ، خصوصا پيوند به بايگاني ها (براي نمونه به سمت راست صفحه راديو نپال آزاد كه نمايش داده شده است مراجعه كنيد) .


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

اين كار براي انتخاب شدن بسيار موثر است زيرا متن موجود در پيوند ها(كه anchors ناميده مي شود)عامل مهمی در ايجاد ارتباط با آن چيزی است كه در جستجوگرها،جستجو شده است. بنابراين در اين مورد،وجود كلماتي چون" state vandalism in Nepal "(ويرانگري دولت در نپال)در اولين پيوند يا عنوان"راديو نپال آزاد"در نهمين پيوند ميزان ارتباط صفحه با كلمات كليدی مورد نظر را به شدت بالا می برد.همچنين صفحه اي كه اين پيوند ها را روي خود دارد(براي موتورهاي جستجوگر صفحاتي كه امكان فشار روي عبارت های آنها وجود دارد اهميت بيشتري دارند) و صفحاتي كه از سوي آنها نمايش داده مي شوند، مرتبط تلقي مي شوند .

چگونگي بالا بردن امكان انتخاب شدن يك وبلاگ

وبلاگ ها ويژگي هاي مفيد دروني زيادي دارند كه ميزان و امكان انتخاب شدن آنها را بالا مي برد . هنگامي كه موتور جستجوگر به واسطه معرفي مكانيكي وبلاگ يا از سوي «عنكبوت»ها - كه به دنبال پيوند ها هستند - شناسايي مي شوند، شانس انتخاب شدن اين گونه وبلاگ ها، به واسطه خواص ذاتی شان، بيشتر از وب سايت‌های استاندارد است. اما براي افزايش قابليت رويت بايد كمي جلوتر هم برويم.
در اينجا نكاتي چند براي رسيدن به اين مرحله با استفاده از كلمات كليدي مهم برگرفته از عنوان وبلاگ شما ذكر مي شود .

۱. روي فناوري هايي تمركز كنيد كه امكان انتخاب شما را افزايش مي دهند

اگر پايگاه الكترونيك شما هنوز On line نشده،در مورد فناوري كه براي اين كار انتخاب مي كنيد(مانند Blogger ، Dotclear ، BlogSpirit ، Joueb و بسياري ديگر)دقت فراوان داشته باشيد. فناوري ای را انتخاب كنيد كه بيشترين جزئيات مربوط به انتخاب شدن را در خود جاي داده باشد :

- عنوان نشريه بايد بطور كامل در صفحه عناوين (the <TITLE> tag) و همچنين در URL بطور كامل باز توليد شود (با توجه به اين كه اين موضوع هميشه اتفاق نمي افتد زيرا در بعضی ابزارها به شكل خودكار بعد از چند كاراكتر، بقيه نام حذف می شود) .
- ايجاد پيوندهاي دائمي (پيوندهاي صفحات حاوي يك متن خاص) بايد امكان پذير باشد .
- فناوري انتخاب شده بايد به شما امكان طراحي بالا و هر چه بيشتر شخصي كردن محيط وب سايتتان را بدهد. يعني شما بتوانيد از طراحي گرافيكي و صفحه بندي شخصي در آن استفاده كنيد . مهارت في شما در اين زمينه بايد تا حدي افزايش يابد كه بتوانيد از بيشترين عوامل موثر در برگزيده شدن پايگاه الكترونيكي خود از سوي موتورهاي جستجو گر استفاده كنيد .

براي كنترل اين موارد بايد به پايگاه هاي الكترونيك كه از اين فناوري استفاده كرده اند،مراجعه كنيد(همواره يك نمونه بارز خوب در آنجا وجود دارد)تا ببينيد كه چگونه نمايش داده مي شوند.با اين روش مي توانيد چيزهاي زيادي را بياموزيد.

۲ . بهترين عنوان را براي مطلب خود انتخاب كنيد

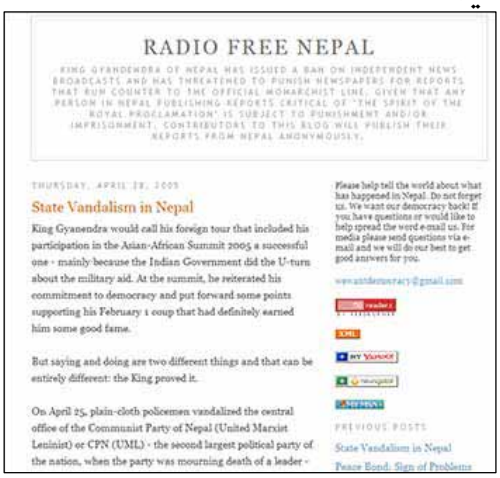
اين نكته بسيار مهم است. عنوان مطلب شما در تك صفحاتي كه نشان گر مطلب هستند، در URL ها و در متوني كه پيوندهاي ارتباطي به متن دارند، باز توليد مي شوند. هر سه آنها مكان كليدي جستجو براي موتورهاي جستجوگر هستند.بنابراين بطور خلاصه مي توان گفت كه عنوان مطالب بايد شامل مهم ترين واژه ها و عبارات باشد تا امكان انتخاب شدن وجود داشته باشد.از انتخاب عناويني چون"چه خوش گفت!" "خوش آمديد!" "عاليه!" پرهيز كنيد. عنوان بايد در قالب كمتر از پنج كلمه بيانگر چيزي باشد كه در متن مربوط به آن بيان شده است.به كلماتي فكر كنيد كه تمايل داريد موتورهاي جستجو به واسطه آنها مطلب شما را انتخاب كنند و از آنها براي تعيين عنوان مطلب استفاده كنيد.اين كار ممكن است چندان آسان نباشد اما بسيار موثر است .

۳ . متن را آماده كنيد

موتورهاي جستجوگر عاشق متون هستند پس برايشان متن آماده كنيد.

مي توانيد تا جايي كه دلتان مي خواهد عكس منتشر كنيد اما فقط در صورتي كه متني نيز همراه آنها درج شود.سعي كنيد كه متن هاي شما حداقل 200 كلمه را در خود جاي دهند زيرا اين كار امكان برگزيده شدن آنها از سوي موتورهاي جستجوگر را افزايش مي دهد.همچنين از درج مضامين مختلف در يک مطلب اجتناب كنيد زيرا موتورهاي جستجوگر از اين كار خوششان نمي‌آيد.قانون طلايي در اينجا،يک مطلب،يک موضوع است.

٤. به اولين پاراگراف نوشته خود توجه كنيد


RADIO FREE NEPAL

KING GYANENDRA OF NEPAL HAS ISSUED A BAN ON INDEPENDENT NEWS BROADCASTS AND HAS THREATENED TO PUNISH NEWSPAPERS FOR REPORTS THAT RUN COUNTER TO THE OFFICIAL MONARCHIST LINE. GIVEN THAT ANY PERSON IN NEPAL PUBLISHING REPORTS CRITICAL OF "THE SPIRIT OF THE ROYAL PROCLAMATION" IS SUBJECT TO PUNISHMENT AND/OR IMPRISONMENT, CONTRIBUTORS TO THIS BLOG WILL PUBLISH THEIR REPORTS FROM NEPAL ANONYMOUSLY.

THURSDAY, APRIL 28, 2005

State Vandalism in Nepal

King Gyanendra would call his foreign tour that included his participation in the Asian-African Summit 2005 a successful one - mainly because the Indian Government did the U-turn about the military aid. At the summit, he reiterated his commitment to democracy and put forward some points supporting his February 1 coup that had definitely earned him some good fame.

But saying and doing are two different things and that can be entirely different: the King proved it.

On April 25, plain-cloth policemen vandalized the central office of the Communist Party of Nepal (United Marxist Leninist) or CPN (UML) - the second largest political party of the nation, when the party was mourning death of a leader -

Please help tell the world about what has happened in Nepal. Do not forget us. We want our democracy back! If you have questions or would like to help spread the word e-mail us. For media please send questions via e-mail and we will do our best to get good answers for you.

www.nepdemocracy@gmail.com

PREVIOUS POSTS

State Vandalism in Nepal

Peace Bond: Sign of Problems

جايگاه كلمات مهم در متن نيز از اهميت بسياري برخوردار است.در مورد پاراگراف اول دقت بسيار داشته باشيد بطور مثال اگر مي خواهيد با كلماتي چون"آزادي اسرا " كه در متن شما به كار رفته است از سوي كاربران انتخاب شويد، سعي كنيد كه در 50 كلمه اول متن خود از اين كلمات استفاده كنيد. شرايط براي ساير كلمات كليدي نيز به همين منوال است.صفحاتي كه در ابتدايشان اين كلمات را در خود جاي داده اند در نتايج حاصل از موتورهاي جستجوگر شرايط بهتري نسبت به صفحاتي داشته اند كه در آنها كلمات كليدي در آخر ذكر شده اند (در حالي كه همه موارد ديگر مشابه باشند).مي توانيد با **برجسته** كردن اين كلمات، آنها را مشخص تر كنيد.اين علائم براي موتورهاي جستجوگر بسيار مهم هستند.

٥ . از درج مجدد متن پرهيز كنيد

همه موتورهاي جستجوگر مجهز به روش هايي براي متن هاي مشابه هستند و اگر 2 صفحه كاملا مشابه باشند تنها يكي از آنها انتخاب شده و ديگري به ندرت در صفحه نتايج،نشان داده مي شود.بطور مثال گوگل اين پيغام را مي دهد:(به منظور نشان دادن بهترين نتايج برخي از ورودي هايي را كه مورد مشابه آنها وجود داشته،حذف كرده ايم.در صورت تمايل مي توانيد جستجو را تكرار كرده و موارد حذف شده را نيز ببينيد.)
اين شرايط براي وبلاگ ها بيشتر پيش مي آيد زيرا صفحات حاوي هر مطلب ممكن است بسيار شبيه به هم باشند. بطور مثال اگر مقدمه اي يكسان براي همه صفحات داريد،يا آن را در پايين صفحه يا تنها در صفحه اصلي ذكر كنيد تا صفحات ديگر قابل تمايز از يكديگر باشند.

٦ . عنوان طولاني براي وبلاگ خود انتخاب نكنيد

بهترين عنوان (محتويات قسمت <TITLE>) براي موتورهاي جستجوگر بين 5 تا 10 كلمه است در صورتي كه كلماتي چون حروف اضافه يا ربط درآن وجود نداشته باشند. عنوان صفحه وبلاگ عموما از 2 قسمت تشكيل شده :

- عنوان كلي وبلاگ
- تكرار عنوان مطلب

بنابراين براي اينكه كلمات در صفحه عنوان اصلي از 10 تا بالاتر نروند بايد براي عنوان كلي وبلاگ و براي عنوان مطلب هر كدام تنها 5 كلمه در نظر بگيريد . اين كار چندان دشوار نيست اما رعايت اختصار در حالي كه اطلاعات هم بطور كلي در آن نشان داده می شوند يكي از نكات كليدي است كه سبب مي شود، موتورهاي جستجوگر وبلاگ شما را انتخاب كنند .

اگر مي توانيد (همه فناوري ها اين امكان را در اختيار شما قرار نمي دهند) ، عنوان مطلب را بالاتر از همه و عنوان كلي را بعد از آن قرار دهيد ، حالت بر عكس آن چندان موثر نيست .

۷ . وبلاگ خود را عضو سنديكاها كنيد

اكثر ابزارهاي وبلاگ نويسي به شما امكان مي دهند كه يك "XML thread" يا "RSS feed" ايجاد نماييد كه به اين وسيله كاربران بتوانند با استفاده از نرم افزاري مناسب متن شما را برداشت نمايند. می توانيد اين تسهيلات را در وبلاگ خود به كاربران ارائه دهيد (نصب آن تنها چند دقيقه طول مي كشد). نه تنها تعداد بازديد كنندگان از وبلاگ شما افزايش می يابد كه كليه بازديد كنندگان Yahoo نيز كه در جستجو به سايت شما برسند، لينك RSS شما را در كنار نتايج جستجو مشاهده خواهند كرد. در شكل زير اين موضوع نمايش داده شده است (View as XML).

بنابراين از اين امكان استفاده كنيد.

۸ . پيوندهاي خود را هميشه روزآمد كنيد

پيوندها بسيار مهم هستند زيرا به موتورهاي جستجوگر اجازه مي دهند تا صفحات سايت را به ترتيب شهرت آنها طبقه بندي كنند.(در Google اين مورد PageRank ناميده مي شود)با استفاده از روش هاي زير مي توانيد تعداد پيوندهاي وبلاگ خود را افزايش دهيد :

- آن را وارد دايركتوری ها كنيد (براي كسب اطلاعات بيشتر به موارد زير مراجعه كنيد) .

جستجو براي پايگاه هاي الكترونيكي كه رقيب نبوده اما مطالبي را در مورد عنواني همسو با وبلاگ شما ارائه مي دهند موثر است.

تبادل پيوندها بين وبلاگ هايي كه علائق و حوزه هاي مشابه دارند بايد به سرعت انجام شود (اين كار در انجمن هاي وبلاگ نويسي مكررا صورت گرفته و پذيرفته شده است و همين امر يكي ديگر از مزاياي وبلاگ ها بشمار مي رود) . وبلاگ ها براي اين كار بسيار مناسبند زيرا حاشيه هاي آنها خالي بوده و به آساني پيوند ها در آن درج مي شوند .

ديده شده در وبلاگ در راهنماي موضوعات

ديده شدن در موتورهاي جستجوگر عمومی (مانند Google، MSN ، Yahoo و Exalead) و راهنماها (مانند Yahoo!Directory و Open Directory) بسيار مهم است اما ديده شدن در موضوعات خاصی نيز اهميت بسياری دارد چرا كه :

- كاربران تخصصی را به وبلاگ شما راهنمايی می كند.
- تعداد پيوندها به وبلاگ شما افزايش مي يابد كه براي حسن شهرت شما مناسب است .
- باعث می شود شما توسط وبلاگ نويسان ديگری كه بر روی همين موضوعات كار می كنند شناخته شويد و احتمال تبادل لينک بالا می رود.

در زير برخي از ابزارهای جستجو (موتورهاي جستجو و فهرست های راهنما) آمده است كه وبلاگ ها را انتخاب مي‌كنند :

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

همچنين به فهرست هر يک از ارايه دهندگان تکنولوژی هم نگاهی بياندازيد، از جمله:

http://www.canalblog.com/cf/browseBlogs.cfm
http://www.dotclear.net/users.html
http://www.blogspirit.com/fr/communautes_blogspirit.html

نتيجه گيري

يک وبلاگ همه عناصر لازم براي انتخاب آسان از سوي موتورهاي جستجوگر را در خود جاي داده است . با نکاتي که در اين بخش ذکر شد و رعايت آنها شما بايد به نتايج خوبي رسيده و قابليت رويت وبلاگ خود را افزايش دهيد. بنابراين راه براي شما باز است و به ياد داشته باشد که " متن پادشاه است " .

***Olivier Andrieu* مشاور آزاد اينترنتي است که تخصص وي در کمك به وبلاگ ها جهت انتخاب از سوي موتورهاي جستجوگر است. پايگاه الکترونيکي زير نيز متعلق به اوست :**
www.abondance.com

چه چیزی باعث درخشش و شهرت یک وبلاگ می شود؟

نوشته مارک گلیسر *

چه چيزي باعث مي شود كه از بين ميليارد‌ها كلمه اي كه توسط ميليون ها وبلاگ نويس در سراسر جهان انتشار مي يابد، تنها يكي از وبلاگ ها مطرح و مشهور شود؟ چه چيزي نويسنده اين وبلاگ را جزو قشر خاصي قرار داده و باعث مي شود كه خوانندگان هر روز به آن مراجعه كرده و نهايتا افتخار و تمجيد رسانه اي را براي او به همراه آورند؟

رابطه، پاسخ اين سوال است. وبلاگ نويسان موفق كساني هستند كه با خوانندگان خود، چه ده نفر و چه ده هزار نفر، بواسطه ايجاد سرگرمي يا اطلاع رساني رابطه برقرار كنند. بسياري از مردم تمايل دارند كه بين وبلاگ نويسان و ديگر نويسندگان (روزنامه نگاران ، رمان نويسان و كساني كه قلمي عامه پسند دارند) حد و مرزي قائل شوند اما هدف اصلی آنها مشترك است: يقه مردم را بچسبيد تا از دستتان فرار نكنند.

برخي از وبلاگ نويساني كه در نوشتن اين كتاب راهنما مشاركت داشته اند – مانند چنعاد بحريني از بحرين ، يان شام شاكلتون از هنگ كنگ و آرش سيگارچي از ايران – در كشورهايي وبلاگ نويسي مي كنند كه دولت با دقت هر چه تمام تر بر كلمات آنها نظارت داشته و اينترنت را كنترل مي كند. ولی از سويي ديگر جهانيان نيز آنها را نظاره می كنند و توسط آن ها از ماجراهايي باخبر مي شوند كه رسانه هاي جمعي اين كشورها جرات بيان آن ها را ندارند. در چنين كشورهايي، آزادي بيان و آزادي مطبوعات در معرض خطر قرار داشته و صداي وبلاگ نويسان On line تنها ارتباط مهم با واقعياتي است كه در كوچه پس كوچه هاي شهر هاي آنها اتفاق مي افتد. عكس هايي كه آنها تهيه مي كنند و داستان هايي كه مي گويند از اهميت بسياري برخوردار است.

اما چه چيزي باعث درخشش هر چه بيشتر اين وبلاگ ها مي شود؟ در زير برخي ويژگي ها آمده است كه باعث تفاوت و تمايز اين وبلاگ ها از ميليون ها وبلاگ ديگر مي شود .

صدايي منحصر به فرد و شخصي

بهترين وبلاگ نويسان با صداي خود سخن می‌گويند، به هويت منحصر به فرد خود افتخار می‌كنند و داستان‌هايي را بازگو مي كنند كه از نظر آنها واقعيت دارند. ايده وبلاگ برگرفته از مجلات On line است

یعنی یك مجله شخصي و بنابراین این نكته مهم را باید همواره به خاطر داشته باشیم كه سبك نوشتن در وبلاگ مانند نوشتن مطالب دانشگاهی یا نوشتن برای رسانه های رسمی نیست. چنعاد بحريني نام مستعار یك وبلاگ نویس آسیایي است كه در كشور عربي بحرین زندگي می‌كند و به همین دلیل نسبت به وقایع و رویدادهاي این منطقه دیدگاهی متفاوت دارد. یان شام شاكلتون یك هنرمند اجرایي است كه مدتی در اقصی نقاط دنیا زندگي كرده و تظاهراتی را علیه مسدود شدن سرویس دهنده وبلاگ TypePad توسط چین صورت داده است – در حالي كه خود چند سال قبل به مقامات چین در فیلتر گذاري شبكه كمك كرده بود.

وبلاگ خود را همواره به روز نگه دارید

سكون و ركود یكی از اصلی ترین مشكلات همه وبلاگ ها است. با توجه به این كه اكثر مردم براي وبلاگ نویسي پولي دریافت نمي كنند، پیدا كردن وقتی برای وبلاگ نویسی در زندگي هر روزه مدتي طول مي كشد. بسیاري از مردم وبلاگ نویسي را شروع می كنند، مدتی به آن ادامه می دهند و بعد دیگر هرگز وقتي براي به روز كردن اطلاعات آن پیدا نمي‌كنند. وبلاگ نویسان برای موفقیت باید مطالب خود را دائما به روز كنند و همچنین همیشه مشغول دنبال كردن موضوعات مورد علاقه خود و وقایع مرتبط باشند. البته این بدان معنا نیست كه برای داشتن یك وبلاگ موفق باید 12 بار در روز مطالب را به روز كرد ولی مشخص است كه یك ركورد چند هفته‌ای به راحتی می‌تواند باعث بي‌علاقگي و از دست رفتن مخاطبان شود.

با خوانندگان خود ارتباط برقرار نموده و آنها را توانمند سازید

یكي از ویژگي‌هاي متمایز كننده وبلاگ، امكان ایجاد ارتباط دوطرفه در آن است. راه هاي بسیاري براي درگیر نمودن خوانندگان وجود دارد كه توسط آن ها مي‌توانید افراد را وارد گفتگو كرده و از بازخوردشان (feedback) استفاده كنید. مي توانید یك نظر سنجي On line بگذارید، آدرس پست الكترونیكي خود را در اختیار خوانندگان قرار دهید یا بخش مربوط به نظرات و پیشنهادات را فعال كنید. جف اویي بخاطر نظري كه یكي از خوانندگانش در مورد مطلبي نوشته بود از سوي دولت مالزي مورد تهدید قرار گرفت. اویی به جاي برداشتن همه پیشنهادات، تصمیم گرفت كه پیشنهادات را مدیریت كند تا مطمئن باشد كه خوانندگان تنها در مورد موضوع مورد بحث نظر می دهند و حاضر به پذیرش پیامدهای آن نیز هستند. او یك وبلاگ چیني زبان به نام The Ferryman را نیز براي ایجاد ارتباط بین وبلاگستان مالزیایي و چیني ایجاد كرده 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. براي انجام اين كار يك روش تعريف شده وجود ندارد اما ارائه گزارش اصيل يا داشتن ديدگاهي خاص نسبت به يك مسئله باعث مي شود كه وبلاگ شما جنبه ای خاص پيدا كند. هنگامي كه در نوامبر سال 2004 يكي از فعالان بحرينی زنداني شد، چنعاد بحريني عكسها و صداي تظاهرات كنندگان در بحرين را در وبلاگ خود قرار داد و در موردی دیگر نیز وبلاگ نویس آرش سیگارچي به علت انتقاد از دولت تندروی ایران و همچنین اعتراض نسبت به دستگيري ديگر روزنامه نگاران، دستگير و به 14 سال زندان محكوم شد. او بعدها با پرداخت جريمه 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 محکومیت اش به سه سال کاهش یافت و در حال حاضر در حال گذراندن محکومیت در زندان است.)**نكته اصلي اين است كه اين وبلاگ نويسان و بسياري ديگر همواره در مقابل قدرت ، واقعيت را گفته و اين جسارت را داشته اند تا بعنوان يك نيروي جمعي در وبلاگستان در برابر مقاماتي كه همواره واقعيات را پنهان كرده اند، بايستند .

***Mark Glaser** ستون‌نويس «بررسی روزنامه‌نگاری On line» (www.ojr.org) است. نشريه اي است كه توسط دانشكده ارتباطات آنبرگ وابسته به دانشگاه كاليفرنياي جنوبي منتشر مي‌شود. او نويسنده‌اي آزاد است كه در سانفرانسيسكو زندگي مي كند. مي توانيد با اين پست الكترونيكي با او تماس بگيريد: glaze@sprintmail.com*

آلمان

ما ازحقوق 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 دیجیتالی را با نام «شبکه رسانه های جدید» پایه گذاری کردم. به مدت پنج سال به ارتقای حقوق مدنی و انسانی در حوزه های دیجیتالی پرداختیم. کنفرانس هایی 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 معدود و مشخصی از کاربران ارسال می‌شد. از سوی دیگر، وبلاگ ها باز و شفاف بوده و فرصت‌های بیشتری را برای تبادل دانش و به اشتراک گذاشتن گزارش‌ها در اختیار کاربران قرار می دهند .

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 گزارش هایم 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 فعالیت های 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 نرم‌افزارهای دیگر را نیز آزمایش کردم. وبلاگ ها امکان ایجاد، ویرایش و نشر سریع متن را با کیفیت مناسب در اختیار من قرار می دهند. چیزی که برای من بیشتر از همه اهمیت دارد،رابط پیوندي است که به من اجازه می دهد 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 دگمه 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 می خوانند 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 می کنم که همه اطلاعات مهم را در netzpolitik.org ثبت کنم که شامل این موارد است: حقوق مدنی و حقوق بشر،دنیاي آزاد نشر متون،دسترسی آزاد و رایگان به دانش،جامعه اطلاعاتی و برقراری توازن در حوزه حق‌چاپ. آزادی بیان و آزادی اظهار نظر،شدیدا تحت تاثیر 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 می دهم 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 ارایه 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 می تواند به شیوه ای فعال از سوی سازمان‌ها و شرکت‌های جامعه‌مدنی مورد استفاده قرار گیرد.من مدیر پروژه و مشاور ارتباطات سیاسی در اینترنت و مبارزات ترویجی اینترنتی و دموکراسی اینترنتی بودم که طبقه‌بندی‌ای جداگانه در وبلاگ ها به شمار می روند.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 می توان در وسعتی گسترده‌تر،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 کنفرانس‌های خود را تهیه کرده و نظر خود را در مورد آنها بیان می‌کنم. 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 می‌کنم. وبلاگ من تبدیل به یک مرکز اصلی در بین جامعه مدنی و شبکه های آلمانی زبان شده که مطالب گوناگونی را برای گروه‌های مختلف اجتماعی تامین می‌کند. همچنین من گاهی از دوستان وبلاگ نویس خود می‌خواهم 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 می‌کنم. 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 می‌کنم تا وبلاگ‌های 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 شهامت کسانی را که تحت رژیم های دیکتاتوری به سر می‌برند و با به روز رساندن وبلاگ خود،زندگی خود را به خطر می اندازند،تحسین می‌کنم.

Markus Bechedahl* 28 ساله،مدیر اجرایی newthinking communication است.این سازمان مسوول فن‌آوری‌ها و راهبردهای بازمتن 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 **چنعاد بحرینی**

من به دو دلیل عمده وبلاگ خود را آغاز کردم : (الف) برایم جالب بود که بدون محدودیت ، موعد 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 مستقیما 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 رسانه‌های دیداری و شنیداری دارند. با این حال، در رسانه‌های 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 (خصوصا از پادشاه و عموی او به عنوان نخست وزیر).

اما اینترنت ابزاری برای افراد است تا بتوانند آزادانه عقاید خود را در سطح عمومي 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 اخیرا،مجددا 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 – خصوصا 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 کرده‌ام تا کاري شبیه به روزنامه‌نگاري انجام دهم.

به این معنا که تا جاي ممکن تلاش کرده ام تا خود در مراسم مختلف (خصوصا راهپیمایي‌هاي 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 فضایي ایجاد شده که در آن مي توان با صداقت در مورد طیف گسترده‌اي از موضوعات صحبت کرد. من از وبلاگ هاي بحریني دیگر چیزهایی آموخته‌ام که هیچگاه نمي‌توانستم این اطلاعات را از جایي دیگر کسب کنم. وبلاگستان بحرین فقط یک جمعیت On line نیست بلکه بسیاري از وبلاگ نویسان بحریني ماهانه جلساتي برگزار مي کنند تا به شکل رو در رو در مورد برخي از موضوعاتي که در وبلاگ ها مطرح مي شوند با یکدیگر گفتگو کنند.

با این حال اکثر فعالیت هاي On line در بحرین در تالارهای گفتگوی On line صورت مي گیرد که زمانی طولانی است فعالیت خود را آغاز کرده اند (مثلا در bahrainonline.org). وبلاگ نویسي هنوز در بحرین پدیده اي رایج نیست اما وبسایت‌های ما هم اکنون نقش «پل‌های ارتباطاتي» را به خود مي گیرند (همانطور که حسین درخشان توضیح داده : http://hoder.vom/weblog/archives/013982.shtml) . با توجه به اینکه اکثر وبلاگ نویسان در بحرین به انگلیسي مي‌نویسند، ما مي توانیم با مردم جهان ارتباط دو سویه داشته باشیم تا از طرف آن‌ها به عنوان یک منبع اطلاعاتي موثق براي درك شرایط واقعي بحرین پذیرفته شویم.

بنابراین، بطور مثال، هنگامي 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 بیانیه اي صادر کرد. فکر مي کنم که توجه جهاني که به سمت این موضوع جلب شده بود نقش بسیار مهمي در تصمیم نهایي دولت براي رهایي این سه نفر پس از چند هفته داشت. بطور کلي مي‌توان گفت که وبلاگ هاي ما انحصار خبری دولت در مخابره اخبار بحرین به جهان خارج را شکسته است.

بطور کلي وبلاگ نویسان بحریني به خاطر مطالبي که مي‌نویسند از سوي دولت با مشکلي مواجه نشده اند اما با آغاز سال جدید شرایط تغییر کرده است. همانطور که قبلا گفته شد سه نفر از گردانندگان تالارهای گفتگوی On line در فوریه به علت درج مطالبي که بیانگر تنفر و انزجار آنها نسبت به دولت بود دستگیر شدند. یکي از این

گردانندگان علي عبدالمام، وبلاگ شخصی خود را نیز دارد. همچنین در ماه آوریل، دولت اعلام نمود که صاحبان همه سایت‌ها باید اطلاعات خود را در وزرات اطلاعات به ثبت برسانند و در غیر اینصورت مورد پیگرد قانوني قرار خواهند گرفت. این مطلب نشان مي دهد که دولت هنوز به خوبي اینترنت و وبلاگ‌ها را درك نکرده و نمي داند که در صورت احساس خطر از سوي نویسندگان On line چگونه باید با شرایط برخورد کند.

چنعاد بحريني كه اصالتا متعلق به آسياي جنوب شرقي است اكنون در بحرين زندگي كرده و وبلاگ خود را در آدرس http://chanad.weblogs.usdot دارد. او ترجيح مي دهد كه گمنام باقي بماند .

ایالت متحده آمریکا

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

***نوشته جی روسن**

هنگامي كه تحقيقات خود را در مورد نحوه وبلاگ نويسي آغاز كردم پاسخ هاي متفاوتي شنيدم. اما بخشی كه مشترك بود اين بود: بايد مقالات كوتاه بنويسي. برخي مي گفتند كه سبك كار چنين است. برخي ديگر نيز عقيده داشتند كه تنها اين شيوه تاثير مثبت دارد و بدبين‌ترين آنها عقيده داشتند كه اين چيزی است كه افراد پر مشغله در حال جستجو در وبسايت‌ها به دنبال آن هستند. همه به من می‌گفتند كه افراد وقت كافي براي مطالعه تحليل هاي طولاني و متفكرانه تو را ندارند.

اين موضوع باعث ترديد من شد. تصميم نداشتم كه مقالات طولاني 2000 كلمه‌اي بنويسم؛ اما هنگامي كه تلاش كردم تا ايده هاي خودم را كه هنوز از زبان ديگران بيان نشده بود در قالب مقالات بيان كنم، اين اتفاق افتاد و و بعد از چند مطلب توجه تعدادی از افراد به وبلاگم جلب شد (البته هنگامي كه بخواهم مي توانم كوتاه بنويسم). ديگر براي من حد و مرزي وجود نداشت: آزاد بودم تا خود موثرترين شيوه را انتخاب كنم و دريابم كه PressThink قرار است چگونه چيزی باشد.

اين كه «مردم وقت ندارند...» از نظر من حرفی بي‌معنا بود و ديگر به آن اطمينان نداشتم. چنين نصايحي باعث مي‌شد كه خودم را محدود كنم و نتوانم آنچه فكر مي‌كنم را بنويسم. اما هدف كلي از شروع PressThink دستيابی به آزادي بود: « وای! اكنون من مجله خود را دارم . اكنون مي توانم آنچه را كه فكر مي كنم بنويسم». علاقه اصلی من بيشتر در حوزه كاربراني بود كه فرصت لازم براي مطالعه عميق را داشتند و تعداد آنها براي من به هيچ وجه مهم نبود.

رويكرد من چنين بود : اين مجله من است، PressThink ... اگر دوست نداريد بازگرديد. به شيوه اي بسيار ظريف و انتزاعي، وبلاگ من بخشي از بازار رسانه‌هاي جمعي را تشكيل داده و در رقابت با سايت‌هايي است كه درباره بازي‌هاي نمايشي، فوتبال و سريال تلويزيونی Law and Order می‌نويسند. البته اين حرف چندان هم درست نيست. PressThink يك شهروند آزاد با فضای داوطلبانه است و لازم نيست مانند يك كنشگر بازاری عمل كند. اين تجربه من در طول چندين سال وبلاگ نويسی است.

باید به خاطر داشته باشید که وب در مسایل متفاوت و گاه متضادی سودمند است.براي اطلاعات مهم و فوری،براي گشت زنی در یک حوزه، براي صحبت و ارتباط دو طرفه و همچنین وسیله‌اي براي دسترسي به اعماق،یک ابزار کمک کننده به حافظه،کتابخانه‌اي در دسترس و یك فیلتر.عدم استفاده از یك وبلاگ براي نوشتن تحلیل‌هاي طولاني تنها به این علت که کاربران این ایده را نمي پسندند از نظر وب احمقانه و از نظر رسانه ها هوشمندانه است.من هم فعال حوزه رسانه‌ای نیستم ! عجیب این است که همیشه سعي مي‌کنم مطالب کوتاه و شیك بنویسم اما آنها همواره تبدیل به مقالاتي طولاني مي‌شوند.تعدادي از خوانندگان نسبت به این موضوع اعتراض داشته‌اند.یکي از متداول ترین چیزهایي که مي گفتند این بود:«کلی کلمه برای یک موضوع اشتباه» و این موضوع بعد از مدتي براي من جالب هم شد.

هر وبلاگ خوبي پیش از آغاز باید یک سوال از وب بپرسد:آیا نیازي 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 عباراتي چون group think مشتق شده است اما گروه در آن عبارت از رسانه است.این عنوان همچنین خلاصه شده دکترین Press Thinking است که نوعی فلسفه رسانه‌ای است و روزنامه‌نگاران با آن زندگي مي‌کنند و حتی مي‌توان گفت که در رسانه‌ها به یک مذهب تبدیل شده است.موضوعاتي هستند که توجه مرا به خود جلب مي‌کنند. تفکر رسانه‌ای چیزي است که من به عنوان نویسنده و منتقد به آن مشغول هستم.حتي زماني که در وبلاگ خود مي نویسم نیز این کار را مي‌کنم.

هدف از این کار ارجحیت دادن به تفکر مطبوعاتي دربرابر رویدادهاي گذرایي است که در مطبوعات رخ مي‌دهد.سپس آن را امتحان مي‌کنیم یا از دیگران مي‌خواهیم این کار را بکنند.این چیزی است که معنای حقیقی این عنوان است.این وبلاگ «درباره» تفکر مطبوعاتي است و همچنین اسبابي براي ایجاد تفکر مطبوعاتي بیشتر است. تصور مي کنم که بسیاري از وبلاگ نویسان وقت زیادي را صرف تفکر و انتخاب درست عنوان وبلاگ خود نمي‌کنند.اما در مورد من، تا زماني که عنوان را انتخاب نکرده بودم،آمادگي لازم براي شروع وبلاگ را در خود نمی‌دیدم.

من تلاش می‌کنم تا انتقاد مبتنی بر ایدئولوژی مطبوعات دیگر را به افراد و سازمان هایي بسپارم که مشتاق به انجام این کار بوده و مهارت بسیاری در آن دارند. PressThink یك وبسایت براي بازبیني 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 نمي کنم اما تفکر مطبوعاتي او را مي نویسم. همانطور که در مقدمه وبلاگ خود نوشته‌ام «تلاش مي کنم تا پیامدهاي 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 می‌زنم و به دنبال مطالب جالب می‌گردم. بعد لینک‌ها را جمع می‌کنم و نوشتن را شروع می‌کنم. یا کسي براي من ايميلي مي‌فرستد كه منجر به ارسال يک مطلب مي‌شود. گاهی هم اتفاقاتي رخ مي دهد كه من حس مي‌كنم خوانندگان وبلاگم مي خواهند نظر مرا در باره آن بدانند بنابراين يک مطلب مي‌فرستم. چيزي كه من در اختيار دارم استفاده از سبك هاي متفاوت به جاي استناد به شيوه هاي تغيير ناپذير است، شيوه هايي كه دائما در حال تغيير و تبديل به روش هایی آسان برای ارسال مطالب به PressThink هستند.

در يک مقاله ساده در PressThink مانند " كناره گيري و مرگ تدريجي روزنامه "
http://journalism.nyu.edu/pubzone/weblogs/pressthink/2005/03/29/nwsp_dwn.html
پنج بخش باید پر شوند: تیتر، سوتیتر، متن، و پی‌نوشت‌ها (یادداشت ها ، واکنش ها و پیوند ها) و پیشنهادها. هر کدام از اینها سبك نوشتاري متفاوتي را مي طلبند. تیتر، می‌گوید که متن درباره چه چیزی است و باید توجه خوانندگان را جلب کند. سوتیتر بیانگر مطلب بوده و شمه ای از داستان متن را ارئه مي دهد. متن همان متن اصلي است كه عموما داراي 1500 تا 2500 كلمه و 20 تا 30 پيوند دارد كه هر كدام به نوبه خود بيانگر بخشی از داستان هستند. بخش پی‌نوشت به ويرايش و پيگيري مباحث گسترده‌تر در وبلاگستان مي‌پردازد كه شامل واكنش ها نسبت به نوشته من است. پیشنهادات آغازگر گفتگوها هستند.

مقاله‌ای در PressThink موفق است که همه بخش هاي آن،در مقابل هم قرار داده شوند و خواننده بتواند ارتباط بین آن‌ها را به درستی درک کند. تا زماني كه واكنش هاي بعدي ، بازخوردها و پيشنهادات به مقاله اضافه نشوند(كه اين كار ، گاه بيش از يک هفته طول مي كشد)مطلب وارد PressThink نمی‌شود. این چرخه یک مطلب در وبلاگ است. هنگامي كه كار مقاله‌ای می‌گیرد (که یکبار می‌گیرد و یکبار نمی‌گیرد)، مقالات تبدیل می‌شوند 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 می‌کند، نداشتم اما با سعی و خطا به آن پی بردم. به همین دلیل است که می‌گویم براي يافتن بهترين شيوه وبلاگ نويسي بايد مدتي با آن كار كنيد.

قبل از این که PressThink را آغاز کنم باید ایده‌هاي خود در مورد روزنامه‌نگاري 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 مي کنند تا بفهمند که من به چه چیزی فکر می‌کنم. تفاوت بسیار بزرگ است. حالا آزادی اندیشه دارم.

***J Rosen** در دانشگاه نیویورك آموزش خبرنگاري داده و از سال **1986** در این دانشکده فعالیت داشته است . او از سال **1999** تا **2005** رییس دانشکده بوده است. وی در شهر نیویورك زندگي مي کند و نویسنده وبلاگي در مورد روزنامه نگاري و مشقات آن است که **PressThink** نامیده مي شود (www.pressthink.org). این وبلاگ اولین بار در سپتامبر **2003** معرفي 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. هنگامي که در سال 1989 این اتفاق افتاد من در تونلي بیرون دفتر خبري زین هوا در هنگ کنگ نشسته بودم که در آن اعتصاب غذایی جریان داشت. ما از دانشجویان چیني حمایت مي کردیم. ما براي آن‌ها و برای خودمان دموکراسي مي‌خواستیم. ما دیگر نمي خواستیم که مستعمره بریتانیا باشیم و همچنین علاقمند هم نبودیم که به زیر سلطه حزب کمونیست برویم. ما آزادي مي خواستیم.

دو یا سه ساعت بعد، صداي اولین تیر را از رادیو شنیدم و به دنبال آن صداي سرود، جیغ و انعکاس هجوم تانك ها از پشت دیوار به گوش رسید. هنگامي که به یکدیگر نگاه کردیم ، اشك بر صورت همگان جاري بود .

همه مي دانستیم که چین در مقابل دموکراسي خواهان از تانك استفاده خواهد کرد اما تا آن لحظه نمی‌توانستیم این را باور کنیم. فکر مي کنم در آن زمان بود که Glutter در ذهن من متولد شد یعني زماني که پایان کار نهضت دموکراتیك را در سال 1989 در حالي که در یك تونل با نورهاي فلورسنت نشسته بودم از رادیو شنیدم. در آن زمان 15 سال داشتم.

مدت کوتاهي بعد از این واقعه با خود عهد بستم. عهدي که کمتر زنان بي تجربه اي مانند من،در دنیا ممکن است جسارت لازم آن را داشته باشند تا با عزمي راسخ از آن صحبت کنند :

" هرگز فراموش نخواهم کرد. قسم مي خورم که تا ابد به یاد داشته باشم. من بخاطر خودم و همه، زندگي بهتري خواهم داشت زیرا من زنده ماندم ولي شما دیگر زنده نیستید. هرگز اجازه نمي‌دهم 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 بي تجربگي این عهد را با خود بستم. هرگز با خود فکر نکردم که چگونه مي توان به این اهداف دست یافت و آیا امکان آن وجود دارد.

اما فكر مي كنم حق با من بود، همه بزرگسالان از درون بلندگو ها همين چيزها را فرياد مي زدند.

تنها امشب به اين نتيجه رسيده ام كه همه اين نوشته ها، عكس‌ها و كارهاي هنري كه به نام دموكراسي انجام داده ام، مقاومت‌های اعتراضی كه در حوزه مجازی سازماندهي كرده ام، مصاحبه‌هايي كه در آن‌ها شركت كرده ام ، و داستان هايي را كه تحت عنوان آزادي بيان منتشر نموده ام نه تنها به خاطر اعتقاد پر حرارت من نسبت به آنها بوده بلكه راهي براي تسكين ضمير نا خود آگاهم نيز هست. وبلاگنويسي باعث مي شود كه به عهد خود نسبت به كساني كه مردند، وفاكنم. علت اين كه اين موضوع را براي شما مي نويسم اين است كه بدانيد چرا Glutter را ايجاد و مديريت كردم. زيرا اين كار به پيروي از هيچ قانون خاصي يا با نسخه برداري از فرد ديگري صورت نگرفته است. من نمي‌خواستم توجه ديگران را به خود جلب كنم و يا شهرتي به هم بزنم. شايد خلوت بودن وبلاگ را ترجيح می‌دهم و هنگامي كه توجه به وبلاگ زياد مي‌شود، مدتی آن را راكد باقي مي‌گذارم چرا كه تنها آن هنگام است كه مي توانم آنچه را كه مي‌خواهم بنويسم و داستانی كه بايد گفته شود را بدون حضور فشارها، به شيوه ای كه دوست دارم نقل كنم.

نصيحت من به كساني كه مي‌خواهند وبلاگي را آغاز كنند اين است: به هيچكس جز خودتان گوش ندهيد. سعي نكنيد با مراجعه به وبلاگ ديگران از آنها تقليد كنيد. با فهرستی از «بايدها» پشت وبلاگ ننشينيد تا سعی كنيد به آن‌ها دست پيدا كنيد. من قوانين بسياری را شكسته ام چرا كه از آن‌ها اطلاع نداشتم و همه چيز نيز به خوبی پيش رفته است.

تنها چيزي كه براي ايجاد يك وبلاگ به آن نياز داريد اراده آغاز آن است.

تنها چيزی كه برای ادامه يك وبلاگ به آن نياز داريد اين است كه سابقه ای از هرآنچه گفته ايد را داشته باشيد.

هر كدام از ما لحظه به روشنی رسيدن از نظر سياسي را تجربه كرده ايم، محركي كه باعث مي شود به گونه‌اي از بي‌عدالتي پي‌ببريم كه بايد اصلاح شود. در غير اين صورت به يك فعال اجتماعی كه ايده ای برای خلق كردن دارد تبديل نشده بوديد.اجازه دهيد كه اين درك، راهنماي شما باشد. اميدوارم كه شما بتوانيد به گونه اي مطالب خود را به ديگران انتقال دهيد كه آنها را نيز تحت تاثير قرار داده و الهام بخش آنان براي مبارزه ای برای تغيير باشيد. اين تنها چيزي است كه امشب مي توانم به شما بگويم .

حالا ساعت 2:33 دقيقه صبح است و من مي توانم صداي شليك گلوله ها را بشنوم. هر سال همين موقع اين صداها به گوش من مي‌رسند. من 15 ساله بودم. سنم براي چنين تجربه‌هايي بسيار كم بود. اما آنهايي كه مردند نيز براي مرگ جوان بودند.

***Yan Sham Shackleton** مي خواهد كه شما هم بدانيد كه او 6 هفته را صرف نوشتن 6 نسخه از اين مقاله نموده و تلاش كرده تا تمام دانش خود در مورد وبلاگ نويسي را منتقل كند و در نهايت به اين نتيجه رسيده است كه زيبايي اين ابزار به آن است كه بيانگر هويت فرد باشد .*

او در وبلاگ خود Glutter.com از سياست و هنر حرف مي‌زند. صراحت كلام و موضع‌گيري شفاف او نسبت به دموكراسي واقعي در هنگ‌كنگ به اين معناست كه وبلاگ او در داخل همواره اسير سانسور است.

ایران

می توانیم آزادانه در وبلاگ ها بنویسیم

***نوشته آرش سیگارچی**

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

براي سال هاي متمادي روزنامه نگاري با محدودیت هایي مواجه بوده است اما با استفاده از فناوري مي توان این موانع را برداشت.

من در کشوري روزنامه‌نگار هستم که موانع و محدودیت‌ها مانع از انجام فعالیت ام مي‌شوند. علاوه بر عوامل درون سازماني که در اکثر سازمان‌هاي رسانه‌اي جهان وجود دارند، اجزاي برون سازماني مانند محدودیت‌هاي قانوني، نفوذ دولت و افراد، حمایت یك جانبه از منابع خبري، گروه‌هاي فشار و سرمایه‌داران نیز نسبت به کشورهاي پیشرفته از نفوذ بیشتري برخوردارند. بنا براین من وظیفه دارم که درباره استقلال کشور خود و انعکاس آن در اخبار واقعي و تحلیل خودم از اخبار فکر کنم. یکي از روش هایي که براي شکستن این موانع انتخاب کردم، وبلاگنویسي بود.

ما مي‌توانیم آزادانه در وبلاگ‌ها بنویسیم. با توجه به این که وبلاگ ها وارد حوزه چاپ یا بیان اخبار در رسانه هاي دیداری و شنیداری نمي شوند، نوشتن در آنها باعث انتشار سریع اخبار و دیدگاه‌هاي مختلف مي‌شود. وبلاگ ها را مي‌توان آژانس‌هاي خبري کوچکي دانست که نویسندگان آن هم نقش خبرنگار را بر عهده دارند و هم نقش سردبیر را..

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

اما وبلاگ هایي که متعلق به روزنامه‌نگاران و هنرمندان یا شخصیت‌هاي سیاسي، اقتصادي، اجتماعي و ورزشي برجسته است، حتي اگر مطالب آن تنها مربوط به زندگي روزمره آنان باشد، به علت ارزش خبري و حسن شهرت آنها مورد توجه قرار مي‌گیرد.

مردم مطالب زيادي را دارند كه مي‌توانند آنها را مكتوب نموده و مخاطبان خود را جلب كنند.
من عقيده دارم كه هر وبلاگي افراد علاقه‌مند به اين حوزه را جلب مي‌كند، بنابراين هيچ محدوديتي در وبلاگنويسي جايز نيست .

من دو روش براي وبلاگ نويسي انتخاب كردم، به صورت غير رسمي و به شيوه عاميانه، نظر خود را در مورد وقايع جاری بيان مي‌كنم. در شيوه دوم اخبار، تحليل، مصاحبه، گزارش يا مقاله مي‌نويسم. اين كار باعث مي شود كه هر دو گروه خوانندگان را جلب كنم يعني كساني كه مي خواهند بدانند هم اكنون مشغول چه كاري هستم و هم كساني كه انتظار دارند بعنوان يك خبرنگار، نويسنده و شاعر ديدگاه‌هاي خودم را بيان كنم.

وبلاگ ها بعنوان ابزاري On line به نويسنده فرصت مي‌دهند تا ديدگاه‌ها و انتقادهای صريح خوانندگان را دريافت كرده، و يا به آنها پاسخ دهد يا خود را اصلاح كند. وبلاگنويس در اين رابطه نزديك با خوانندگان، اين امكان را دارد كه با ابراز ديدگاه‌ها يا نوشتن مطالبي كه خواننده از آن لذت مي‌برد، آنها را در جهت درست سوق دهد.
همانطور كه قبلا گفتم اگر مي خواهيد كتاب،شعر،داستان،روزنامه يا مجله‌اي در ايران چاپ كنيد بايد از مقامات مجوز بگيريد.بسياري از نويسندگان و روزنامه نگاران به خاطر اين قانون دچار مشكل شده اند.
اگر بخواهيد داستان، شعر يا مقاله‌اي را در روزنامه يا مجله‌ای چاپ كنيد، سانسور مي‌شود. بنابراين بسياري از نويسندگان ايراني ديدگاه‌هاي خود را با هزينه كمتر و بدون تجربه كردن فشار سانسور در وبلاگ ها منتشر مي كنند . به همين دليل دولت ايران نيز همانند چين و ديگر نقاط جهان استفاده از اينترنت را محدود مي كند.

روزنامه نگاري اينترنتي باعث پيشرفت آزادي بيان و گسترده‌تر شدن ديدگاه‌ها مي‌شود. اگرچه از سوي دادگاه‌هاي ايراني محكوم شده‌ام اما اميد خود را از دست نداده و مطمئن هستم كه در سالهاي آينده مقامات كشورم به نشر آزاد اطلاعات و آزادي بيان احترام خواهند گذاشت.

*آرش سيگارچي ، روزنامه نگار و وبلاگ نويس ، در سال 1978 يعني دوران انقلاب و براندازي شاه به دنيا آمده و در سال 1993 يعني در 15 سالگي كار روزنامه‌نگاري را آغاز كرده است. زماني كه در سال 1997 رئيس جمهور اصلاح طلب جناب آقاي محمد خاتمي انتخاب شد او به مطبوعات اصلاح‌طلب پيوست. بعد از آن در آوريل سال 2000 كه اين رسانه ها توقيف شدند، او براي زندگي به شمال ايران رفت و در آنجا سردبير يك روزنامه 12 صفحه‌اي به نام «گيلان امروز» شد.

او در سال 2001 در يك وبلاگ گروهی به نام «گيله مرد» كار خود را آغاز كرد. در سال 2002 آرش سيگارچی پايگاه الكترونيكي خود به نام «پنجره التهاب» را شروع كرد. (www.sigarchi.com)

در اوايل سال 2005 از سوي وزارت امنيت و اطلاعات به مدت 2 ماه بازداشت شد و سپس به 14 سال زندان محكوم گرديد. او هم اكنون آزاد و منتظر دادگاه تجديد نظر است.(رجوع شود به توضيحات صفحه 34)

نپال

دنیای خارج را از وقایع داخلی مطلع می‌سازیم

*رادیوی نپال آزاد

در تاريخ اول فوريه 2005 پادشاه جيانندرا بر اريكه قدرت نشست و مردم از طريق يک سخنراني تلويزيوني از آن مطلع شدند. هنگامي كه سخنراني به پايان رسيد، مي خواستم واكنش هاي بين المللي اين تغيير و تحول را بدانم و بنابراين تلاش كردم به اينترنت متصل شوم. رايانه پيغام داد كه هيچ خط تلفني به آن متصل نيست. فهميدم كه خطوط تلفن قطع شده‌اند. شاه برای جلوگیری از درز هرگونه خبر از نارضایتی مردم به خارج، به ارتش دستور داده بود كه نه تنها مراكز ارائه دهنده خدمات اينترنتي را ببندد بلكه خدمات مخابراتي را نيز قطع كند.

در طول اين مدت مردم در مورد پيامدهاي مختلف اين حركت صحبت كرده و حتي برخي اين حركت شاه را تحسين مي‌كردند. در دفتر روزنامه اي كه من در آن كار مي كردم همه آينده‌اي تاريک را پيش رو مي ديدند زيرا مطمئن بودند كه كاركنان ارتش به درون اتاق هايخبري تلويزيون نفوذ كرده و اخبار را سانسور خواهند كرد. آن هنگام بود كه فكر كردم نوشتن وقايع روزانه و افكار مردم به شكل يادداشت‌های مجزا اقدامی مناسب است. اين كار را با استفاده از رايانه انجام دادم.

در تاريخ 8 فوريه خدمات اوليه مخابراتي و اينترنتي مجددا فعال شد. بسياري از افراد با ارسال پست الكترونيك از من مي‌خواستند كه وقايع نپال را براي آنها توضيح دهم. در آن زمان تصور كردم كه يادداشت هاي روزانه من مي توانند به بهترين نحو شرايط را تشريح كنند. برخي از دوستانم در ايالات متحده آمريكا به من پيشنهاد كردند كه يادداشت‌های هر روز را با تنظيم تاريخ روی روز نوشته شدن يادداشت‌ها، به اينترنت بفرستم. از آنجايی كه من در امور وبلاگ نويسي كمي مبتدي بودم، آن‌ها اين كار را برای من كردند. تصميم گرفتم گمنام باقی بمانم و از ديگر دوستانم هم بخواهم كه بدون اسم واقعی در وبلاگ‌ها بنويسند تا به اين ترتيب از امكان رويارويي با دولت و آزار و اذيت و زندان در امان باشيم.

سانسورهاي شديد رسانه هاي جمعي در اولين روزها و تبادل آزاد اطلاعات در راديو نپال آزاد، باعث شهرت روز افزون اين پايگاه شده و Blogger.com نيز مردم را دعوت به ديدن اين سايت می‌كرد. دوستان من در ايالات متحده آمريكا نهايت تلاش خود را براي شهرت هر چه بيشتر اين سايت كردند. طي چند هفته، سايت كاملا مشهور شده بود.

علت ايجاد راديو نپال آزاد و هدف اصلی انجام چنين كاري اين بود كه مردم سراسر دنيا از احساسات تك تك مردم در مورد حكمراني شاه با خبر شوند. رسانه هاي جمعي كه تحت سانسور شديد قرار داشتند، تنها بايد مطالب طبع ميل پادشاه را مي‌نوشتند و در نتيجه هيچ يك توان انعكاس احساسات واقعي مردم را نداشتند. اگر چه راديو نپال آزاد حاصل تلاشی يك نفره و نيز مشاركت گاه به گاه چند تن ديگر بود اما به خوبي توانست بدون سانسور و بدون ترس از آزار و اذيت دولت، احساسات مردم را بيان كند.

مطالب اوليه راديو نپال آزاد بيشتر به صورت يادداشت هاي روزانه بوده و رويدادهاي روز را تشريح مي كردند. ورودي‌هاي جديدتر با تفكر و تحليل وقايع همراه شده‌اند. در شرايط سياسي نپال كه پادشاه بدون در نظر گرفتن انتخاب مردم به زور قدرت را بدست گرفته است، راديو نپال آزاد از اهميت بالايي برخوردار است زيرا به مركز بيان افكار عمومی تبديل شده است.
در حقيقت چيزي كه در كشورم به دنبال آن هستم، دموكراسی است چرا كه معتقدم اين تنها راه شكوفايي كشور است و چيزی است كه به شغل من به عنوان يك روزنامه‌نگار معنا می‌دهد. نوشتن در شرايط سانسور مثل نوشيدن قهوه بدون شكر است، بی‌مزه! ما به عنوان يك روزنامه‌نگار، از چيزهايي اطلاع داريم كه برای نوشته شدن هرگز جايی در روزنامه‌ها پيدا نمی‌كنند. مثلا يكي از اخباري كه در راديو نپال آزاد درج شد در مورد اكتساب دارايي هاي شخصي به شيوه‌اي ناشايست از سوي شاه بود. بسياري از روزنامه‌نگاران از اين موضوع خبر داشتند، از آن انتقاد می‌كردند و درباره‌اش شوخی می‌كردند ولی هيچ جايی نبود كه درباره آن بنويسند.

يكي ديگر از اهداف كه راديو نپال آزاد توانست به آن دست يابد ، اطلاع رساني در مورد شرايط داخلي نپال به سراسر دنيا بود. اگر راديو نپال آزاد به وجود نمي‌آمد ممكن بود كه هزاران هزار نفر از مردم دنيا نسبت به شرايط نپال بي اطلاع بمانند. فكر مي‌كنم كه اين روش براي بر انگيختن افكار مردم در سراسر جهان بسيار مناسب بوده است.

پيشرفت هاي الكترونيك كمك شاياني به جامعه ما كرده‌اند. من آزادانه و بدون ترس مي‌نويسم زيرا مطمئن هستم كه شيوه وبلاگنويسي من - يعني نوشتن مطالب و ارسال آنها از طريق پست الكترونيك به دوستانم در ايالات متحده براي نشر - بدون استفاده از شيوه‌هاي بسيار پيچيده قابل پيگيري نيست. هنگامي كه دموكراسي به كشور بازگردد و مردم آزادی داشته باشند ، من احساس غرور خواهم كرد زيرا خواهم دانست كه در رسيدن به آن نقش داشته‌ام.

خیلی‌ها با ارسال پست الکترونیک درباره اعتبار نوشته‌هایم از من سوال کردند. به آنها گفتم که یك نام نمي تواند مقیاس خوبي براي سنجش اعتبار باشد. نمي خواهم که تا زمان طلوع دموکراسي در نپال نام خود را فاش کنم زیرا ممکن است شرایط رو به و خامت گذاشته و من بخاطر وبلاگ نویسي راهي زندان شوم. از زندان نمي ترسم 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 حمایتتان تشکر مي کنم .

وبلاگ نویس رادیو نپال آزاد ، نپال
wewantdemocracy@gmail.com
رادیو نپال آزاد وبلاگي است که علیه قدرت مطلق پادشاه جیانندرا و علیه سانسور رسانه‌هاي جمعي مقاومت می‌کند. رادیو نپال آزاد براي بازگرداندن دموکراسي به کشورش فعالیت می‌کند و اطلاعات به روز درباره شرایط داخلي 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 فني و سریعی است برای وبلاگنویسي گمنام. رویکرد این نوشته بررسی وضعیت در کشوری است که در آن دولتی غیرشفاف ممکن است به تعقیب وبلاگنویسان بپردازد. این راهنما براي سایبرپانک‌ها نوشته نشده بلکه برای حمایت از افرادی نوشته شده که در کشورهاي 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

معرفي سارا

سارا به عنوان حسابدار در یك دفتر دولتي كار مي كند. او متوجه شده كه رییسش، یعنی معاون وزیر، پول هنگفتی از دولت اختلاس كرده است. او مي خواهد جهانیان را درباره جرمی كه واقع شده مطلع كند اما نگران از دست دادن شغلش است. اگر این موضوع را به وزیر گزارش دهد (البته اگر بتواند وقت ملاقاتي بگیرد !)، ممكن است خودش اخراج شود. او با یكي از خبرنگاران روزنامه محلي تماس مي‌گیرد اما خبرنگار مي‌گوید كه بدون در دست داشتن اطلاعات و اسناد كافي براي اثبات این ادعا، امكان درج آن در روزنامه‌ها وجود ندارد.

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

وقتی سارا سعی می‌کند که به شکل گمنام وبلاگ بنویسد، دو شیوه وجود دارد که ممکن است منجر به لو رفتن‌اش بشود. اول این که او هویت خود را از طریق مطالبي که منتشر مي کند فاش نماید – بطور مثال اگر در یکی از مطالب بنویسد: «من دستیار مدیر ارشد بخش حسابداري معاون وزیر صنایع و معادن هستم» عملا 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 رایانه اي که به اینترنت وصل مي شود داراي یك نشاني است که آن را IP مي‌نامند. 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. هنگامي که سارا از مرورگر اینترنت خود برای ارسال یک نظر در وبلاگ وزیر استفاده می‌کند، آدرس IP او به همراه مطلب‌اش ثبت می‌شود.

با کمي تلاش ، کارشناسان فني رایانه اي وزیر مي توانند این نشاني را دنبال کرده و به هویت سارا پي ببرند. اگر سارا از رایانه خانگي‌اش استفاده کند تا با خط تلفن به یک مرکز ارائه دهنده خدمات اینترنتی (ISP) متصل شود، به احتمال قوي این سرویس دهنده نشاني IP اختصاص شده به سارا، شماره تلفن و ساعت کار او را ثبت میکند. در برخي کشورها، وزیر ممکن است برای گرفتن این اطلاعات نیاز به دریافت یک مجوز رسمی داشته باشد ولی در بعضی کشورهای دیگر (خصوصا کشورهایي که ISPهایش متعلق به دولت هستند) این اطلاعات به آسانی در اختیار دولت قرار خواهند گرفت و سارا به دردسر خواهد افتاد.
شیوه هاي گوناگوني وجود دارد که سارا می‌تواند با استفاده از آن‌ها هویت خود را مخفي کند. به عنوان یک قانون کلی، هرچقدر که خواهان ایمنی بالاتری باشد، باید تلاش بیشتری هم انجام دهد. سارا یا هر کس دیگري که مي خواهد به صورت گمنام وبلاگ نویسي 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 برخي از راهکارهایي که به منظور پنهان کردن هویت On line به کار مي روند به دانش و تلاش فني زیادی نیاز دارند.

گام اول – نام‌هاي مستعار

ساده ترين روشي كه سارا براي پنهان كردن هويت خود مي تواند استفاده كند، به كارگيري يک سرويس ايميل رايگان و يک سرويس وبلاگنويسی رايگان خارج از كشور است. (استفاده از سرويس‌های پولی ايده جالبی نيست چرا كه با پيگيري نحوه پرداخت دولت می‌تواند به شماره كارت اعتباری سارا يا اطلاعات حساب PayPal او پی ببرد و از اين طريق به سادگی هويت او را آشكار كند). سارا به آساني مي تواند هويت جديدي براي خود انتخاب كند – يك نام مستعار – و براي وارد شدن به سرويس‌های مورد استفاده‌اش از اين نام مستعار استفاده كند. حالا وقتی كه وزير وبلاگ او را ببينند، اسم A. N. Ymous را به عنوان نويسنده خواهد ديد كه از ايميلی با آدرس anonymous.whistleblower@hotmail.com استفاده می‌كند.

برخي از ارائه دهندگان شناسه‌های رايگان ايميل عبارتند از:
Hotmail
Yahoo
Hushmail – ايميل رايگان مبتنی بر وب با حمايت خوب از رمزگذاری

برخي از ارائه دهندگان سرويس وبلاگ مجانی عبارتند از :
Blogsom – وبلاگ هاي رايگان مبتنی WorldPress
Blogger
Seo Blog

اشكال اين روش كجاست؟اشكال اينجاست كه وقتی سارا براي استفاده از خدمات پست الكترونيكي يا وبلاگنويسی وارد سايت سرويس دهنده می‌شود، نشانی IP او در آنجا ثبت مي‌شود. اگر امكان پيگيري اين نشاني IP وجود داشته باشد – اگر او از رايانه خود در خانه يا محل كار استفاده كند و اگر شركت ارائه كننده خدمات پست الكترونيكي يا وبلاگ مجبور به ارائه اين اطلاعات به دولت باشد – هويت سارا فاش خواهد شد. البته اجبار شركت هاي خدماتي شبكه جهاني براي ارائه اين اطلاعات بطور مثال hotmail ، جهت يافتن نشاني IP سارا بسيار دشوار است و جناب وزير براي اين كار بايد احتمالا از طريق سازمان مجری قانون ايالات متحده آمريكا مجوز كسب كند. اما به هرحال سارا علاقمند نيست در اين مورد ريسک كند.[2]

[2] توجه داشته باشيد كه در ايران بر اساس قانون، كليه ISPها مجبور هستند كليه ارتباطات كاربران خود را ثبت كنند و در صورت نياز آن را در اختيار دولت قرار دهند. پس اين شيوه از كار در ايران نيز ايمن نيست.

گام دوم - رايانه هاي عمومي

اقدام ديگري كه سارا مي تواند براي پنهان كردن هويت خود استفاده كند، استفاده از رايانه‌هايي است كه عموم مردم از آن استفاده مي‌كنند. او مي‌تواند بجاي اين كه حساب‌های کاربری وبلاگ و ايميل خود را از رايانه خانه يا محل كار تنظيم كند، به كافي‌نت‌ها، كتابخانه‌ها يا دانشگاه‌ها مراجعه كند. در اينصورت وقتی جناب وزير نشاني IP يك مقاله يا اظهار نظر را پيگيري كند، تنها به كافي‌نتي خواهد رسيد كه روزانه تعداد زيادي از مردم از رايانه‌هاي آن استفاده مي‌كنند.

البته اين روش هم مشكلاتی دارد. اگر كافي‌نت يا مركز رايانه كتابخانه يا دانشگاه نام و زمان افرادی كه از كامپيوترها استفاده می‌كنند را ثبت كنند، هويت سارا آشكار خواهد شد. او نبايد نيمه شب از اين مراكز استفاده كند زيرا تعداد مراجعه كنندگان كم بوده و فرد مسوول كامپيوترها ممكن است چهره او را بخوبي به خاطر بياورد. در عين حال او بايد همواره كافي‌نت محل مراجعه خود را تغيير دهد چرا كه اگر جناب وزير متوجه شود كه همه مطالب افشاگرانه از كافی‌نت Joe’s Beer and Bits در فلان خيابان ارسال شده‌اند كافی است يک نفر را برای زيرنظر گرفتن مشتريان در آن حوالی بگذارد و بعد از يک هفته به هويت سارا پی‌ببرد.

گام سوم – Proxy هاي گمنام

سارا از اين كه بايد برای درج هر مطلب به كافی‌نت Joe مراجعه كند خسته شده است. او با كمک كاردان كامپيوتری كه همسايه‌اش است رايانه‌اش را برای استفاده از يك Proxy گمنام تنظيم می‌كند. حالا هر وقت كه بخواهد می‌تواند به پست الكترونيک و وبلاگش دسترسی داشته باشد. از اين به بعد هر وقت كه از ايميل يا وبلاگ‌اش استفاده كند يا در جايی نظری بنويسد، شماره IP پروكسی سروری باقی خواهد ماند كه به آن متصل است و نه شماره IP واقعی خودش؛ به اين ترتيب كار يافتن او براي جناب وزير بسيار دشوار مي‌شود.

در ابتدا او بايد فهرستی از پروكسی‌های On line بيابد، اينكار به سادگی با جستجو به دنبال عبارت Proxy Server در گوگل عملی است. سارا برای اينكار به سايت publicproxyservers.com مراجعه می‌كند و يكی از پروكسی‌هايی كه با عبارت «گمنامی بالا» (High Anonymity) مشخص شده است را انتخاب می‌كند.

برخي فهرست‌های پروكسی‌های قابل اطمينان برای استفاده عموم عبارتند از:

- Publicproxyservers.com – پروكسی‌های گمنام و غير گمنام
- Samair (http://www.samair.ru/proxy/) – تنها پروكسی‌های گمنام و همچنين شامل اطلاعاتی درباره پروكسی‌هايی كه از SSL پشتيبانی می‌كنند.

- 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 می توانید 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 SSLی 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 مستقیما 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 لااقل 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 آمده اید.

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 مطمئنا 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 بوده اند. 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 دقیقا در همان لحظه از آن پروکسی استفاده کرده است. سارا برای غلبه بر این مشکل از پروکسی‌های مشهور استفاده می کند و دائما 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 پروکسی ها 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 معمولا 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 برنامه‌هایی است که مردم می‌توانند از طریق آن پروکسی‌هایی 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 می‌کند. کار نصب آن چندان هم آسان نیست. اول باید Perl را روی رایانه‌اش 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 اینصورت لازم خواهد بود تا هربار که سارا می‌خواهد از پروکسی استفاده کند، او کامپیوترش را روشن کند. دوست سارا نرم افزار را آماده کرده، سپس با تلفن همراه سارا تماس می‌گیرد و URL ی را که سارا می تواند از طریق آن وارد سیستم پروکسی شود را به او می‌گوید. حالا سارا می‌تواند 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 کافی‌نت 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 می‌کند همواره مشکل پیدا می‌کند و باید روشن و خاموش شود. هر وقت این اتفاق می افتد، سرویس دهنده اینترنت جیم یک IP جدید را به رایانه او اختصاص می‌دهد و در نتیجه هربار که این جریان تکرار می‌شود، 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 می‌شود. 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 می کند که سارا از Tor استفاده کند که سیستمی نسبتا 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 می گیرد 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 می شناسد. 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 فن‌آوری، 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 می‌بیند 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 دائما 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 می رسد 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 عملا غیر ممکن است.

چیزی که بیشتر او را نگران می سازد این است که Tor گاهی از کار می‌افتد. علاوه بر این به نظر می رسد 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

حتما 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 خبره 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/Publi-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 می دهد 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 قبلا «کلید عمومی» اش را در اختیار سرویس دهنده قرار داده بود، سرویس دهنده می‌توانست اولا 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 عملا 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 شخصا آن را کمپایل کند؛ این احتیاج به کلی کمک از طرف یک نفر خبره 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 هربار 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 معمولا برای درک مفهوم کلیدهای عمومی و خصوصی مشکل پیدا می‌کنند. البته ابزارهای خوش‌دست‌تری هم برای رمزگذاری GPG وجود دارند؛ مثلا 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 واقعا 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 ارسال کننده‌های ناشناس مجدد باشد. اگر کسی بخواهد از نسخه جدیدتر استفاده کند یا برنامه را روی سیستم‌عامل‌های لینوکس یا مک استفاده کند باید شخصا 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 ارسال کننده‌های مجدد تحت وب دریافت کند، کار بسیار آسان‌تر می‌شد ولی در حال حاضر من این سرویس را سرویس چندان مفیدی برای کسانی که واقعا 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، شاهدی 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 شدیدا رمزگذاری شده است – مشکوک بوده و ممکن است باعث بررسی دقیق‌تر فعالیت‌های سارا شود.

گمنامي تا چه حد لازم است؟ در اين بحث تا كجا بايد پيش 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 معمولا 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 رسانه های جمعی سنتی خصوصا در کشورهای در حال توسعه است. او بنیانگذار و رئیس سابق **Geekcorps** است که سازمانی غیرانتفاعی است و در زمینه آموزش فن‌آوری 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

فن‌آوری 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 عموما 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 ماهیتا 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 هرزه 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 نرم افزارهای فیلترگذاری امکان بررسی On line فیلتر بودن یا نبودن URL ها 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 معمولا متعلق به احزاب سیاسی مخالف یا روزنامه‌ها، سازمان‌های حقوق بشری، ارائه دهندگان اخبار بین‌المللی و متون انتقادی علیه دولت هستند. کشورهای سانسورگر معمولا 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 فن آوری ها توسط شرکت‌های خصوصی طراحی شده است و برخی دیگر نیز توسط هکرها و فعالان اجتماعی. طیف آنها بسیار گسترده است و برنامه های 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 می دهد و شخصی که از آن استفاده می‌کند. ارایه 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 می شوند. 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 توازنی 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 کاربرانی 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 ارایه کنندگان و کاربران آن باید به این سوالات پاسخ دهند:

تعداد کاربران احتمالی و پهنای‌باند موجود چیست؟ (برای ارائه کننده و کاربر فن‌آوری دورزدن)
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 دورزدن)
کاربر نهایی چه رابطهای قابل اعتمادی در خارج از کشور دارد؟
مجازات احتمالی کاربرانی که در حین استفاده از فن آوری دورزدن 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 پهنای‌باند 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 پهنای‌باند بسیاری اشغال شود. بنابراین، ممکن است بخواهید دسترسی به دورزننده خود یا میزان پهنای‌باند مجاز در هنگام استفاده از آن را محدود نمایید. فن‌آوری های مختلف موجود، برخی یا همه این گزینه‌ها را در اختیار شما قرار می‌دهند.

محل 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 استفاده 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 دورزننده‌ها بیشتر می‌شود. موانع پیش روی کاربران غیر فنی شامل نصب و راه‌اندازی برنامه‌ها و همچنین اجرای تنظیمات و بعضی تغییراتی است که لازم است هنگام استفاده از فن‌آوری دورزننده صورت گیرد. این مساله هم در مورد ارایه کننده سرویس صادق است و هم استفاده کننده آن. استفاده نادرست از فن آوری 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، گزینه‌هایش 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 دورزننده در تماس باشد و راه حلی پیدا کند که دقیقا 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 دور زننده‌ها 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 دورزننده‌های 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 می دهد، 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.
سیستم های 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 عموما محدود به ترافیک وب (HTTP) بوده و معمولا به شکل رمزگذاری شده (SSL) قابل دسترسی نیستند. همچنین سرویس‌های تحت وب (مثلا ایمیل تحت وب) که نیازمند ورود به شبکه باشند نیز معمولا در این روش قابل دسترسی نخواهند بود.
سرویس‌های دورزننده تحت وب عمومی معمولا به خوبی شناخته شده‌اند و ممکن است از سوی مقامات مسدود شده باشند. در حال حاضر اکثر این سرویس دهندگان توسط نرم‌افزار های 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 ارایه 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.guardster.com
http://www.unipeak.com	http://www.webwarper.net
http://www.anonymizer.ws	http://www.proximal.com
http://www.proxyweb.net	http://www.the-cloak.com

از آنجایی که این سایت‌ها در همه جا شناخته شده هستند، اکثر نرم‌افزارهای فیلترگذاری تجاری و همچنین اکثر کشورهای فیلتر کننده اینترنت در حال حاضر آن‌ها را در فهرست سایت‌های فیلتر شده قرار داده‌اند. اگر آدرس این سایت‌ها در فهرست باشند، نمی‌توانید از سرویس‌های آنان استفاده کنید. همچنین بسیاری از سرویس‌دهندگان عمومی دورزننده‌ها، ترافیک ارسالی به کاربر نهایی را رمزگذاری نمی‌کنند. پس این احتمال وجود دارد که داده‌هایی که برای این سرویس‌دهنده‌ها ارسال یا از آن‌ها دریافت می‌شود، توسط افراد مسوولین دورزننده‌ها شنود شوند.[3]

استفاده از دورزننده‌های عمومی تحت وب برای کاربرانی مناسب است که در شرایط کم خطر کار می‌کنند و آشنای قابل اعتمادی در نقاط بدون سانسور ندارند و تنها می‌خواهند 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 نرم‌افزارهای دورزننده تحت وب ممکن است نیاز به مهارت فنی و منابع مناسب (مانند یک سرویس دهنده وب و پهنای‌باند) باشد. با استفاده از دورزننده‌های خصوصی، محل دورزننده فقط در اختیار استفاده کنندگان آن باقی می‌ماند در حالی که در صورت استفاده از دورزننده‌های عمومی، هم کاربران به آدرس آن دسترسی دارند و هم مسوولین فیلترگذاری (و در عین حال اکثر نرم‌افزارهای تجاری فیلترگذاری نیز این آدرس‌ها در فهرست سانسور خود قرار داده‌اند). احتمال ردیابی، کشف و بسته شدن دورزننده‌های تحت وب خصوصی بسیار کمتر از سرویس‌دهنده‌های 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 دور زننده روی آن کار می‌کند و اضافه کردن رمزگذاری. Secure Sockets Layer یا SSL پروتکلی است که توسط آن اطلاعات رمزگذاری شده در اینترنت منتقل می‌شوند.

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

این قابلیت عموما 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 نمی تواند 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 ارایه 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 گزینه ها 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 ارایه 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 می توان 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 بی کاربر 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. شدیدا 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 ارایه 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 درصورت 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 عملا خطری نداشته باشد. اگر کاربران بتوانند از «انگشت نگاری» یا امضای ایمن سند SSL برخوردار شوند، این امکان برایشان به وجود می‌آید که شخصا صحت و اعتبار صفحه دریافت شده را بررسی کنند و درنتیجه در مقابل حملات «آدم در وسط» ایمن شوند.[4]

پروکسی سرورها

«پروکسی‌سرور» سرویس دهنده ای است که بین یک سرویس‌گیرنده (مثلا مرورگر وب) و سرویس‌دهنده (مثلا وبسایت) واسط می‌شود. پروکسی سرور مانند یک حافظه میانجی (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 ضعف های احتمالی سیستم دورزننده فیلترهای اینترنتی) در http://peacefire.org/circumventor/list-of-possible-weaknesses.html و پاسخ پل بارانوسکی در 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 می رسد ولی ممکن است در مکان‌های عمومی مانند کتابخانه‌ها، کافی‌نت‌ها و یا حتی محل کار امکان پذیر نباشد.

مزایا:
بسته‌های نرم‌افزاری مختلفی وجود دارند که می‌توان توسط آن‌ها پروکسی‌های نامریی 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 ا ز 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 زننده‌های 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 گونه‌ای تنظیم کرد که پاسخگوی نیازهای سیستم های فیلترگذاری محیط‌های خاص باشند.

- Squid یک نرم افزار پروکسی سرور است که می‌توان 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 توانایی‌های فیلترگذاری بالا است که می‌تواند 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 می‌دهد تا از پروکسی HTTP که دسترسی اینترنت شما را مسدود می‌کند، رد شوید.

پروکسی سرور های شخصی با قابلیت رمزنگاری بهترین شیوه برای گروه‌ها و کاربرانی هستند که در محیطی اداری به یک دورزننده دائمی و پایدار نیاز داشته و همچنین به رابط قابل اعتمادی که دارای مهارت‌های 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

پروکسی‌های باز، سرورهایی هستند که یا به عمد یا برای ارتباط با کامپیوترهای راه‌دور باز گذاشته شده‌اند. معمولا معلوم نیست که آیا پروکسی‌های باز برای سرویس‌دهی به عموم مردم باز گذاشته شده‌اند یا به علت اشتباه در تنظیمات باز هستند و مردم می‌توانند از آن‌ها استفاده کنند.

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

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 پروکسی های 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 پورت‌ها 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

مسایل امنیتی مرتبط با پروکسی سرورها

تنظیمات پروکسی سرورها از اهمیت ویژه‌ای برخوردار است زیرا امنیت و گمنامی استفاده کنندگان کاملا به آن وابسته است. علاوه بر عدم استفاده از رمز نگاری، 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.

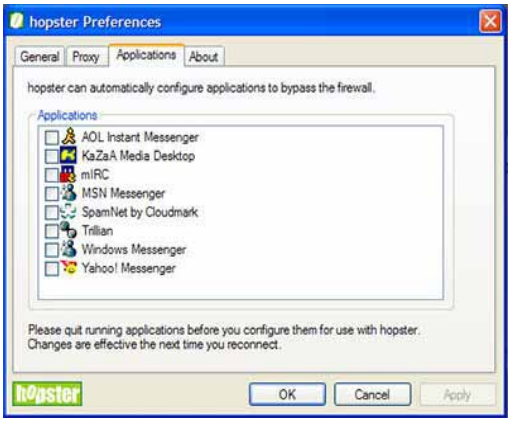
جستجو به دنبال پروکسی‌های آزاد و استفاده از آن‌ها هم پیشنهاد نمی‌شود. این پروکسی‌ها معمولا به دلیل در دسترس بودن استفاده می‌شوند و با وجود کارایی آن‌ها در دور زدن فیلترهای اینترنتی، قابلیت‌های امنیتی خوبی ندارند.

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 می دهند 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 اینترت بررسی می‌شود. [5]

استفاده از پروکسی سرورهای باز و قابل دسترسی برای عموم، معمولا 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

تونلزدن



تونل زدن، که به «port forwarding» هم شناخته می‌شود به افراد اجازه می‌دهد که ترافیک غیرایمن 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 معمولا دارای تبلیغ هستند. درخواست نمایش این تبلیغ‌ها معمولا به شکل متن ساده صورت می‌گیرد و در نتیجه مسوول بازرسی می‌توانند از روی آن‌ها حدس بزنند 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 معمولا 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.
تونل زدن 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 ارایه کننده‌های 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 تحمیلی 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 لااقل تا حدی امکان نصب برنامه بر روی آن‌ها را دارد. کسانی که از طریق رایانه‌های عمومی مانندکتابخانه ها 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 سیستم های ارتباطی گمنام مواجه شوند. اگر سیستمی که استفاده می شود 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 عموما قابلیت پروکسی کردن ایمن بسیاری از پروتکل‌ها، و نه فقط وب، را فراهم می‌کنند.
آنها عموما دارای اجتماعی از کاربران و توسعه دهندگان هستند که می‌توانند به افراد کمک‌های فنی ارایه 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 نرم‌افزارهای 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 تونل های مجازی است که به مردم و گروه ها 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 شبکه های 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 نرم افزار آزاد و رایگان است که به شما اجازه می‌دهد اطلاعات را بدون نگرانی از سانسور بر روی شبکه منتشر کنید یا دریافت کنید. این نرم افزار کاملا غیر متمرکز بوده و ناشران و کاربران اطلاعات کاملا گمنام هستند.
http://freenet.sourceforge.net

استفاده از چنین سیستم هایی ممکن است نیاز به مهارت‌های فنی بالایی داشته باشد.
سیستم های 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.

نتیجه گیری

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. دولت ها 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 ارایه 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 می کند، 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 اخیرا بر روی **OpenNet Initiative (ONI)** 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 می شود. **Nart Villeneuve** فارغ التحصیل دانشکده تحقیقات **Peace and Conflict** از دانشگاه تورنتو است.*

با تشکر
Michelle Levesque ، Derek Bambauer و Bennett Haselton

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 بین المللی 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 تضمین کننده ایمنی ایمیل نیستند. صاحبان شبکه‌هایی که پیام‌های شما از آنها عبور می‌کنند، می توانند 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 می شوند یا باید به زور وارد سرور آن‌ها شوید یا پیام‌های در حال انتقال را شنود کنید، کاری که از نظر فنی مشکل‌تر است. متاسفانه 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 می‌کنند. بعد از این پیام‌هایشان را با استفاده از این کدها و کلیدها مبادله می‌کنند.

نقص این روش این است که اگر نفر سومی پیام‌هایی که طی آن‌ها میشل و «آن» مشغول مبادله کد و کلید رمزگذاری هستند را شنود کند، خواهد توانست از آن‌ها برای بازگشایی دیگر پیام‌ها و حتی ارسال پیام‌های 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. جزییات کلید رمزگذاری (یا «کلید عمومی») را می‌توان بدون نگرانی روی اینترنت ارسال کرد چرا که نمی‌توان از آن برای رمزگشایی پیام‌ها 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 می‌دهد و یک کلید خصوصی که پیش خودش نگاه می‌دارد). «آن» کلید عمومی خود را برای میشل می‌فرستد و میشل با استفاده از آن، پیام‌هایی که می‌خواهد به «آن» بفرستد را رمزگذاری می‌کند. میشل هم با جفت کلید خودش همین کار را می‌کند؛ کلید عمومی را برای «آن» می‌فرستد و کلید خصوصی را برای رمزگشایی استفاده می‌کند. حالا «آن» و میشل می‌توانند در کمال امنیت، پیام‌هایشان را مبادله کنند.

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

یک کلید آزمایش اعتبار نشده ممکن است یک کلید تقلبی از سوی شخص سومی با نیتی پلید باشد که رمزگذاری را بی‌اثر می‌کند. 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 نرم‌افزار برای ایجاد و استفاده از جفت کلیدهای نامتقارن و مدیریت کلیدهای عمومی دیگران، GnuPG (GNU Privacy Guard) است. این برنامه هم با نرم‌افزارهای ایمیل، مانند «تاندربرد» و «آوتلوک» کار می‌کند و هم با ایمیل‌های تحت وب و هم با برنامه‌های چت.

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

***Ludovic Pierrat** مهندس کامپیوتر گرداننده Wa است؛ شرکتی در زمینه تولیدات ومشاوره فن‌آوری 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 عموما نیز این کار توسط فن‌آوری‌هایی صورت می‌گیرد که از شرکت‌های آمریکایی خریداری شده است. چین در این امر بسیار پیش رفته 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 نمی تواند 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.

پکن 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 «براندار» - 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 مثلا حاوی جستجوی تلفیقی «تیانانمن» و «فاجعه» باشند را شناسایی و دسترسی به آن‌ها را محدود کند.

این حکومت قادر است که انجمن‌ها و تالارهای گفتگوی اینترنتی را نیز تقریبا بلافاصله سانسور کند. نرم‌افزارهای هنرمندانه و پلیس حوزه های 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 پیشرفته ای دست پیدا کرده در حالی که تنها یک دهه قبل هیچ شرکت اینترنتی بزرگی در این کشور فعالیت نداشت؟ با کمک شرکت های بزرگ امریکایی که تحت مدیریت Cisco قرار دارند. این شرکت ها 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 نمی کنند، برخورد بسیار خشنی دارند. هفتاد و پنج نفر از مخالفان که تلاش نموده‌اند در حوزه های 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 دیدگاه های سختتری دارند، قابلیت‌های اقتصادی و فن‌آوری همسایه خود را به دست نیاورده‌اند. 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 می رسد که جامعه بین المللی به این نتیجه رسیده که عملکرد تونس در سطح محلی قابل قبول است زیرا اتحادیه ارتباطات مخابراتی بین المللی 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 می رود بسیار ناراحت کننده است.

ایران : جوخه مرگ

سانسور اینترنتی در آسیا تنها از سوی رژیم های کمونیست اعمال نمی‌شود. سیستم فیلترگذاری در ایران طی سالهای اخیر بسیار پیشرفت کرده و وزارت طلاعات[منظور وزارت اطلاعات و فناوری اطلاعات(وزارت پست و تلگراف و تلفن سابق)]ادعا می‌کند که اخیرا راه دسترسی به صدها هزار وبسایت را مسدود کرده است. ملاهای 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 وبلاگ نویس 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 رئیس جمهور 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 می‌دانند 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 رسانه‌های سنتی شدیدا کنترل می‌شوند. چرا مردم از این موضوع خبر ندارند؟ احتمالا پاسخ این سوال، افسانه قدرت همیشگی انقلاب کوبا است.

عربستان سعودی : اهداف مشخص

مقامات عربستان سعودی آشکارا می‌پذیرند که اینترنت در کشور آن‌ها سانسور است. البته در آنجا، مانند چین با Page not found مواجه نمی‌شوید بلکه به صفحه‌ای می‌روید که می‌گوید 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 می‌توانند از طریق آن،سایت‌های جدیدی که فکر می‌کنند باید سانسور شوند را پیشنهاد کنند. واحد خدمات اینترنتی می‌گوید که هدف از بستن این وبسایت‌ها حمایت شهروندان علیه مضامین توهین آمیزی است که اصول اسلامی و هنجارهای اجتماعی را نقض می‌کنند. 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 وبسایت‌های مخالف در این کشور امکان پذیر نبوده و خبرنگاران اینترنتی همواره مورد تهدید و تهاجم فیزیکی قرار می‌گیرند .

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

راهنمای

وبلاگ نویسان

برای

مقابله با سانسور

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. 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. 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 خطر نا خشنودی دولت و گاه بازداشت را به جان می خرند.

این کتاب راهنما برخی نکات فنی را در مورد نحوه راه اندازی یک وبلاگ خوب ارائه می دهد . اما داشتن وحفظ 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 .

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

Printed August 2005, France.

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