

Dictatorships get to grips with Web 2.0

Background paper prepared by Julien Pain, Head of Internet Freedom Desk, Reporters sans Frontières

New Media: The Press Freedom Dimension. Challenges and Opportunities of New Media for Press Freedom. Sponsored by the World Press Freedom Committee, co-sponsored by UNESCO, in partnership with the Coordinating Committee of Press Freedom Organizations, and the The John S. and James L. Knight Foundation.
Paris, 15-16 February 2007

A decade ago, regime opponents in Vietnam or Tunisia were still printing leaflets in their basements and handing them out to fellow militants at clandestine meetings. Independent newspapers were no more than a few hastily-stapled photocopies distributed secretly.

These days, “subversive” or “counter-revolutionary” material goes on the Internet and political dissidents and journalists have become “cyber-dissidents” and “online journalists.” Most of them know how to create a blog, organise a chat group, make phone calls through a computer and use a proxy to get round censorship.

New technology allows them to receive and share news out of sight of the authorities. The Web is also a blessing for human rights groups, which can now build a file on a political prisoner with a few mouseclicks instead of over weeks and sometimes months. The Web makes networking much easier, for political activists as well as teenagers. Unfortunately, this progress and use of new tools by activists is now being matched by the efforts of dictatorships to fight them. Dictators too have entered the world of Web 2.0.

Sixty people are currently in jail for posting criticism of governments online, with China’s 50 making it by far the world’s worst prison for cyber-dissidents. The Chinese have been aped by other countries - four such dissidents are in jail in Vietnam, three in Syria and one each in Tunisia, Libya and Iran.

Parliaments in these countries, along with the local cyber-police, closely follow the latest technological developments. When instant messaging, such as MSN Messenger, became all the rage, China asked the firms that made these programmes to automatically block some key-words, making it impossible for Chinese users to talk about the Dalai Lama and Taiwanese independence, for example.

And with the success of YouTube, China and Iran are keen to filter the videos that appear there - too much “subversive” content for China and too much “immorality” for Iran. In Vietnam, police and dissidents chase play cat-and-mouse with “chat rooms” and three people were arrested there in October 2005 for discussing democracy on Paltalk, a US website that organises remote meetings. One of them, Truong Quoc Huy, was still in prison at the end of 2006.

Spyware that filters e-mail

The Internet was not designed to protect message confidentiality. It is fast and fairly reliable but also easy to spy on and censor. From the first mouse-click, users leave a trail and reveal information about themselves and what their tastes and habits are. This data is very valuable to commercial firms, who sort through it to target their advertising better.

The police also use it. The best way to spy on journalists a few years ago was still to send a plainclothes officer to stand outside their house. This can be done more cheaply and efficiently now, because machines can spy, report back and automatically prevent subversive conversations.

Cuba has installed spyware in cybercafé computers so that when users type “banned” words in an email, such as the name of a known political dissident, they see a warning that they are writing things considered a “threat to state security” and the Web navigator then immediately shuts down.

The Internet giants work with the dictatorships

The predators of free expression are not all the same. China keeps a tight grip on what is written and downloaded by users and spends an enormous amount on Internet surveillance equipment and hires armies of informants and cyber-police. It also has the political weight to force the companies in the sector - such as Yahoo!, Google, Microsoft and Cisco Systems - to do what it wants them to, and all have agreed to censor their search-engines to filter out websites overcritical of the authorities.

This makes the regime’s job very much easier because these firms are the main entry-points to the Internet. If a website is not listed by these search-engines, material posted on them has about as much chance of being found as a message in a bottle thrown into the sea.

Not all countries are strong enough to make the US multinational Internet firms bend to their will, but all authoritarian regimes are now working to censor the Web, even countries in sub-Saharan Africa. The Ethiopian regime of prime minister Meles Zenawi has blocked openly-critical websites and blogs since May 2006 and Zimbabwean President Robert Mugabe is considering a law allowing security forces to intercept online messages without reference to the courts. One of the first moves by Thailand’s military rulers after their September coup was to censor news websites, even foreign ones, that criticized the takeover.

When a dictator cannot effectively censor the Internet, he can take a more radical approach - barring Internet access to virtually everyone, as in North Korea and Turkmenistan. And when a tyrant dies, as Turkmenistan’s “President-for-Life” Saparmurad Nyazov did in December, his successor starts work by declaring his policy towards the Internet. These days, dictators talk about the Web when they want to show their regime is progressive.

Internet users are organising themselves and conjuring up new solutions to tackle these dictatorships, get round the filters and protect their anonymity. They use and create new technology, encrypt their email and use other tools that are still not detected by cyber-police.

The Web phone service Skype, for example, has made it much easier for journalists - and Reporters Without Borders - to communicate with their sources. It works especially well because it is encrypted and so conversations are hard to tap. But China has already signed an agreement with Skype to block key-words, so how can we be sure our conversations are not being listened to? How do we know if Skype will not also allow (or already has allowed) the Chinese police to spy on its customers?

It has become vital to examine new technology from a moral standpoint and understand the secondary effects of it. If firms and democratic countries continue to duck the issue and pass off ethical responsibility on others, we shall soon be in a world where all our communications are spied on.

Create your blog with Reporters Without Borders and read our "blog review" : www.rsfblog.org .