Ministry of Foreign Affairs of the Netherlands

Protecting and supporting cyber activists

Background paper

Introduction

Freedom of expression, as laid down in article 19 of the Universal Declaration of Human Rights (UDHR), and the freedom of association and assembly are important conditions for building democratic societies based on the rule of law. In our modern information age, the Internet has become one of the key channels through which people can exercise these rights.[1] It is the primary means of seeking and imparting information, especially for people living under authoritarian regimes. Furthermore, services like social networks, user-generated content sites and blogs help activists to get organised, develop and share their views, and focus the world's attention on the situation in their country.

To limit the power of the Internet in supporting these key rights, authoritarian regimes have turned to censorship and use blocking and filtering techniques to stem the free flow of information. Authoritarian regimes also employ the Internet to crack down on activist movements, for instance through monitoring and surveillance, hacking and physical persecution of Internet users. In fact, the Internet does more to enable ubiquitous and fine-grained surveillance than any other form of communication. So, while it may act as a countervailing force against the power of authoritarian regimes, we must also recognise that the Internet can adversely affect activist movements.[2]

Initiatives aimed at protecting and furthering internet freedom in oppressive regimes are for the most part aimed at enabling open access to information on the Internet, supporting the activities of (cyber) activists, and protecting them against surveillance. Governments, civil society, the private sector and academics the world over are engaged in projects supporting and strengthening the efforts of cyber activists. Examples include providing circumvention tools against censorship and anonymisation tools to counter surveillance, conducting research and reporting on Internet censorship practices, and organising training projects to ensure that cyber activists are able to use these new tools as safely as possible

In this paper we will give an overview of different initiatives in the area of protecting and strengthening the efforts of cyber activists.

1 LaRue, F. (2011), Human Rights Council , Seventeenth session , Agenda item 3, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue, 16 May 2011
2 Morozov, Y. (2011), The Net Delusion: The Dark Side of Internet Freedom, New York: Public Affairs

The threat to cyber activists

In states where people are not entirely free to speak, the Internet is a vital tool for seeking and imparting information. In Belarus, for example, the Internet is the key source of objective information, as most independent newspapers have been closed down and media is state controlled.[3] The Arab Spring has shown that the Internet can help activists in authoritarian regimes to get organised and exchange views. Furthermore, social media and user-generated content platforms have enabled thousands of bloggers and journalists to publish information and keep the international community focused on the situation in their country.

But while the Internet may act as a countervailing force against the power of an authoritarian regime, we must also be aware that the Internet can adversely affect activist movements. The reason for this is that the Internet can strengthen the three most important tools wielded by authoritarian regimes: censorship, surveillance, and propaganda.[4] In particular, censorship and online surveillance threaten the freedom of expression online. In an effort to control the free flow of information, authoritarian regimes have cracked down on cyber activists and have taken significant steps to limit the access to information on the Internet.[5]

The reasons why states engage in online censorship and surveillance can be divided into roughly four broad categories, *viz.*, for political gain, to curb civil disorder, to protect national security, and to technically limit the capacity for Internet use.[6] A number of different tools and mechanisms are currently used by authoritarian regimes to control the online activities of their citizens. These include blocking content, filtering Internet content, and manipulating Internet search results. States have even gone so far as to shut down the Internet and phone services entirely. In other places regimes and their proxies have hacked and sabotaged websites in order to silence dissenting voices. Furthermore, states may employ online monitoring technologies and hacking tools to eavesdrop on confidential communication. Finally, they can track the digital footsteps of journalists, bloggers and other cyber activists in order to harass them offline through intimidating, arresting or persecuting them, threatening their employment, or ensuring that they disappear.

3 Puddephatt, A., Horner, L., Hawtin, D. (2010), *Information and Communication technologies and Human Rights*, *European Parliament DG External Policies of the EU*, June 2010, p. 29; see also: Kalinoskayva, T. (2010), *Opposition attacks Belarus Internet crackdown*, AFP, 2 February, 2010

4 Morozov, Y. (2011), The Net Delusion: *The Dark Side of Internet Freedom*, New York: Public Affairs

5 It is relevant to note that regimes that limit online freedom are faced with the so-called 'Internet Dictator's Dilemma': by limiting the free flow of information to maintain power and stability, the regime also cuts itself off from the rest of the world socially and economically, which in turn might also threaten the stability and power of the regime. However, given the scale on which censorship and surveillance takes place throughout the world, the Dictator's Dilemma in itself does not seem to be a sufficient deterrent for authoritarian regimes.

6 Puddephatt, A., Horner, L., Hawtin, D. (2010), *Information and Communication technologies and Human Rights*, *European Parliament DG External Policies of the EU*, June 2010

Supporting and protecting cyber activists

Societal actors worldwide are undertaking a number of initiatives to combat the threats of online censorship and surveillance.[7] In this section we give an overview of different activities undertaken by these actors. Many of these efforts are specifically aimed at supporting and protecting cyber activists.

State efforts

As the primary actors responsible for ensuring the freedom of citizens and the protection of their fundamental rights on a national and international level, governments play a central role in protecting and furthering internet freedom. Supporting activists in countries with authoritarian regimes by ensuring an open Internet, while at the same time protecting them against surveillance, is therefore an important feature of modern human rights and foreign policy.

This conference takes place against the backdrop of growing restrictions by repressive regimes on online freedom.[8] Several governments have publicly expressed concern about state-sponsored limitations to freedom of expression online. At the international level, various states have undertaken significant initiatives to respond to modern day restrictions on internet freedom.

The key policy goal is to place internet freedom firmly on the international agenda and create international agreements and standards for internet governance through multi-stakeholder dialogue.[9] As well as initiatives at policy level, states also fund programmes that offer concrete aid to cyber activists. Below are some examples of countries that have projects in place for supporting and protecting them.

The United States

Since 2008, the US State Department has committed over 70 million dollars to a range of internet freedom initiatives. These include support for censorship circumvention technologies, training in online security for cyber activists, funding for the protection of independent websites in countries like Iran, development of secure communications tools for computers and mobile phones, and support for research and advocacy that advances online freedoms.[10] Furthermore, the United States supports independent journalists and activists through the Civil Society 2.0 initiative, which connects civil society actors with technology, thereby strengthening the impact of their efforts.[11]

7 See also the background paper on the role of government and the background paper on corporate responsibility
8 See for example the *Global Internet Filtering* Map by OpenNet Initiative http://map.opennet.net/filtering-pol.html
9 For more information on this topic see the background paper on the role of governments in promoting internet freedom
10 For an overview see: Moloney Figliola, P., Addis, C. L., Lum, T. (2011) U.S. *Initiatives to Promote Global Internet Freedom: Issues, Policy, and Technology,* Congressional Research Service
11 www.state.gov/statecraft/cs20/index.htm

Sweden

Strengthening the freedom of expression throughout the world is an important aspect of Sweden's foreign policy. In 2011, more than three million euros were allocated for promoting and strengthening internet freedom. Projects are mainly funded through development funds. Examples include establishing an activist blog to increase the space for freedom of expression, enabling the safe exchange of information between human rights organisations in Central America, and providing internet security solutions for online media in countries with repressive regimes.[12] Furthermore, the Swedish International Development Cooperation Agency (SIDA) has sponsored APC's 'Connect Your Rights' Campaign and the further development and operation of the TOR project.[13,14]

The Netherlands

In the Netherlands, internet freedom is also a priority in human rights foreign policy. The Netherlands supports projects aimed at strengthening media diversity and promoting human rights from the Human Rights Fund. A significant part of the total budget is allocated for projects related to internet freedom.[15] Initiatives in this area are aimed at: 1) training in online journalism, 2) creating awareness of secure online behaviour, 3) use of circumvention tools and 4) offering strategic hosting support. By using this approach the Dutch government has for instance supported media diversity in Iran, trained online journalists in Afghanistan to make them aware of online security, and made direct investments in projects that offer proxy servers to online activists.[16]

13 www.sweden.gov.se/sb/d/3214/a/179192
14 www.torproject.org/about/sponsors.html.en
15 In 2011 the total budget of the Dutch Human Rights Fund was EUR 35.8 million
16 Letter to the House of Representatives on internet freedom, 2010 - 2011 session, 32 500 V, no. 191 (in Dutch only)

Civil society efforts

Civil society actors help protect and support cyber activists in a number of ways.[17] First of all, NGOs raise awareness about limitations on press and internet freedom throughout the world by providing benchmark studies. Initiatives in this area include the Freedom House *Freedom on the Net Report*, the Open Net Initiative *Internet Filtering Map*, and the Reporters Without Borders *Press Freedom Index*. [18] Civil society actors, for example Access and Human Rights Watch, also lobby for more international action against oppressive regimes that stifle internet freedom. Furthermore, they engage in multi-stakeholder dialogue with the private and public sector in order to further internet freedom.

In addition to policy-oriented approaches designed to promote and advance internet freedom, NGOs also provide direct support to activists, for instance by raising awareness on internet security, providing blogging platforms and training in online journalism. Examples of NGOs active in this area are Cyberdissidents.org, Global Voices, Hivos and the Association for Progressive Communication (APC).

Another area in which civil society is active is the protection of cyber activists. To protect cyber activists, civil society actors help develop and distribute anonymisation- and censorship-circumvention technologies and services. TOR (The Onion Router) is the most well-known of these technologies.[19] TOR is an anonymisation service that allows users to hide the source and destination of their internet traffic. Other examples of services aimed at circumventing Internet censorship are Psiphon, Freegate and Ultrasurf. [20]

Academic efforts

Many universities promote internet freedom. A notable example is Harvard University's Berkman Center for Internet and Society, which has conducted research on the use of Internet circumvention tools.[21] The Berkman Center is also responsible for the Global Voices project, which has evolved into an NGO with over 200 participating bloggers.[22] Other key institutions active in this area are George Washington University in Washington, D.C. and the Oxford Internet Institute.[22,23] The academic world's contributions also include generating an inventory of best practices in the field of promoting free speech online, and helping identify tools and actors that can be effective in support of cyber activists.

17 It must be noted that the examples given in this section represent only a small fraction of the NGOs and initiatives aimed at protecting and supporting the efforts of cyber activists
18 See: www.freedomhouse.org; http://map.opennet.net/ and http://en.rsf.org/press-freedom-index-2010,1034.html
19 www.torproject.org
20 www.psiphon.ca; www.dit-inc.us; www.ultrasurf.us
21 cyber.law.harvard.edu/research/circumvention
22 www.globalvoicesonline.org
23 www.law.gwu.edu/News/20112012events/Pages/SpeakerSeries.aspx

Private sector efforts

As well as governments, the private sector is a key actor in the debate on protecting and supporting activists and in helping bring this about. After all, most of the infrastructure and services that make up the global Internet are in the hands of the private sector. The response of private sector actors to requests from authoritarian governments to monitor, filter and block information flows and/or to relinquish personal data, directly impacts the efforts of cyber activists. An important development in this regard is the Global Network Initiative (GNI), in which leading technology companies, investors and academics have adopted joint principles on freedom of expression and privacy, as well as guidelines for dealing with censorship and/or surveillance requests from governments.[25] Furthermore, the sale of monitoring, filtering and blocking technologies to authoritarian regimes may also affect cyber activists.[26] Corporate social responsibility also features prominently in this area.

In addition to corporate social responsibility, the private sector also contributes to internet freedom and protecting and strengthening cyber activists by sponsoring organisations like Global Voices and the TOR project.

Individual efforts

Last, but certainly not least, there are a large number of independent individuals and groups supporting the efforts of cyber activists. These individuals and groups are themselves often current or former cyber activists, and share their experience and/or provide platforms for other dissidents to use. Examples include Nawaat.org and CyberACT.[27] A growing number of Internet experts and hackers are also involved in protecting and supporting cyber activists.

25 www.globalnetworkinitiative.org/cms/uploads/1/GNI_-_Principles_1_.pdf
26 For an overview of this debate see the background paper on corporate social responsibility
27 www.nawaat.org; www.arabcyberact.org

Conclusions

The Internet offers enormous potential for journalists, bloggers and activists. In countries where freedom of expression, association and assembly are limited, the Internet has become the primary means to exercise these rights. Authoritarian regimes in many countries see the Internet as a threat and actively engage in online censorship. Moreover, authoritarian regimes use the Internet to monitor the activities of cyber activists and track them down. As such, the Internet also poses new threats to activists.

Throughout the world societal actors (state, civil society, academia and private sector) are engaged in supporting and protecting cyber activists. These efforts include raising awareness about limitations to internet freedom, training cyber activists in online journalism and secure use of the Internet, and providing censorship- and surveillance-circumvention tools.

Ministry of Foreign Affairs of the
Kingdom of the Netherlands
P.O. Box 20061 | 2500 EB The Hague