Can the Internet be switched off ?

1. Background

The theme of the *resilience* of the Internet is being hotly discussed at present, *resilience* being the capacity of the Internet to continue to function even in the presence of breakdowns or deliberate attacks.

Breakdowns may be due to a hardware failure but also to a software bug. Attacks may be conducted by a small group of vandals, militants, or criminals, but they may also be carried out by a State trying to prevent its people from accessing the Internet, or a part of it.

So is the Internet reliable? Will it withstand the next breakdown? Can three people in a garage stop the Internet? Given the importance that the Internet now has in everyday life, these are crucial questions.

2. Analysis

Several spectacular breakdowns or attacks hit the headlines in 2009-2010. The media treatment of these breakdowns or attacks was generally of the sensational type. The fact of the matter is that the breakdowns or attacks had very limited consequences in space (affecting a single country or a single Internet service) or time.

It is very easy to *disrupt the Internet*, but it is very difficult to create a *global* disturbance lasting more than a few hours. As Pierre Col has said, "The Internet is globally strong and locally weak". It is very easy to disrupt the Internet because it has no mechanisms for military-grade security: the purpose of the Internet is to enable communication, including between people who do not know each other, which implies a level of openness making it vulnerable. But it is very difficult to stop the Internet over the long term because it is truly alive, with operatives who act, correct, replace, and deploy new systems, such that disturbances have always come to a quick end. For example, the censorship of Wikileaks only lasted a short while, showing the capacity of the Internet to repair itself. Making procedures more rigid and increasing the level of control, therefore, would only exacerbate the problem instead of solving it, since it would prevent these intelligent reactions from taking place.

Nevertheless, the increasing dependence of our society on the web, as well as the growing sophistication of the attacks and technological developments are such that it would be unwise to rely on that finding alone. Many efforts are therefore being undertaken at every level to improve the *resilience* of the Internet. Examples include the deployment of DNSSEC[1] in 2010, the efforts made by France's cyber-defence authority (ANSSI) to convene Internet stakeholders on the issue of resilience, the work of the

1 Used to to verify the authenticity of DNS information

Internet Engineering Task Force (IETF)[2], among other things, in order to secure routing, etc.

However, the difficulty of projects such as these must be measured: the value of the Internet is precisely its openness, and to deploy security systems that would make the Internet slow and laborious to use might cure the disease but kill the patient – in particular since the Internet's openness and lack of centralisation are precisely the strengths on which its resilience depends.

In the specific case of the DNS, the operators of this service are continuously occupied with collecting data, analysing attacks, detecting vulnerabilities, and sharing information among themselves within the Operations, Analysis, and Research Centre (OARC) www.dns-oarc.net/>.

The registry for the *.fr* TLD, AFNIC, has implemented a range of resilience techniques, based in particular on the variety of software used for its name servers[3], on the use of multiple service providers hosting the servers, and the like. Hopefully, no inappropriate filtering measures will weaken the construction www.lepoint.fr/high-tech-internet/l-afnic-s-inquiete-pour-l-avenir-d-internet-14-02-2011-1295076_47.php>.

3. Find out more

- **Two vivid stories on cut-off due to hardware failure**: www.zdnet.fr/blogs/infra-net/le-viticulteur-la-tractopelle-et-les-reseaux-39758040.htm> and www.mail-archive.com/frnog@frnog.org/msg13825.html>. Another example is the accidental cut-off that hit Egypt in 2008 www.renesys.com/blog/2008/12/deja-vu-all-over-again_cables.shtml>. Hardware failures only have a very local impact, however; the real danger comes from possible software failures which, because of their lack of diversity, could cripple much of the Internet.

- **An example of a software failure which could have had serious consequences was the "Attribute 99" case** www.bortzmeyer.org/bgp-attribut-99.html>.

- **Internet cut-off by the government in Egypt:** www.bortzmeyer.org/egypte-coupure.html>. This illustrates the power of a local dictator in a country where there are few connections. Is it possible in France? See www.01net.com/www.01net.com/editorial/527741/couper-internet-en-france-possible-ou-pas/>.

-**Technique used by the libyan government to curb and cut off access to the Internet:** www.lemonde.fr/technologies/article/2011/03/07/quatrieme-jour-de-coupure-d-internet-en-libye_1489281_651865.html

- **Analysis of the China Telecom blunder in April 2010** bgpmon.net/blog/?p=323> A stark article, far removed from *Die Hard*. An example of frenzied propaganda, based on the same blunder, can be found here www.foxnews.com/politics/2010/11/16/internet-traffic-reportedly-routed-chinese-servers/>.

About AFNIC

(Association Française pour le Nommage Internet en Coopération)

Non-profit organization, AFNIC is in charge of the administrative and technical management of the *.fr* (France) and *.re* (Reunion Island) Internet domain names. AFNIC brings together public and private members: representatives from the French government, Internet users and Internet Service Providers (Registrars). **Further information.**

2 The main standards organisation for the Internet
3 BIND and NSD