

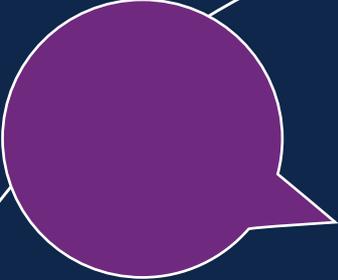


ISSUE PAPER

CAN THE INTERNET BE BROKEN?

afnic

ISSUE PAPER



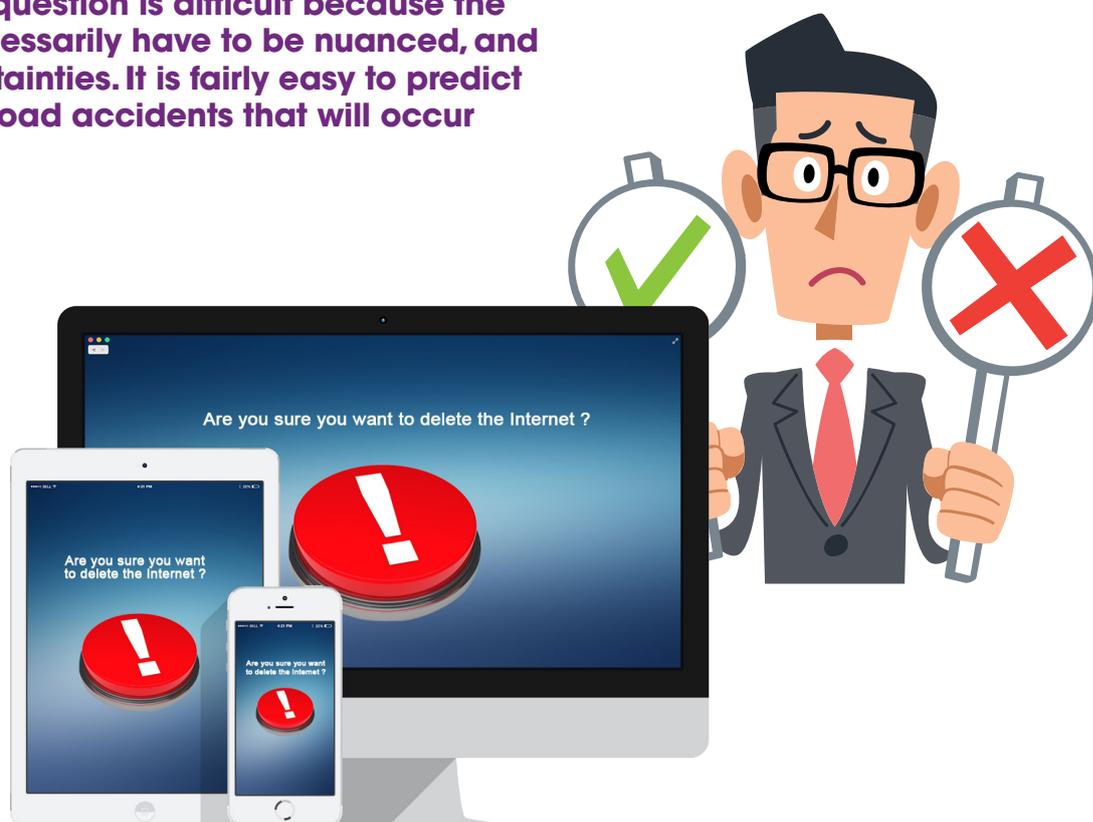
Spectacular incidents, such as the blackout resulting from the attack on Dyn on October 21, 2016, sometimes lead people to believe that it is possible to break the Internet, that is to say to interrupt its operation for a relatively long period. The outage could be the result of a deliberate attack, or an accidental failure.

Sensationalist media have already published articles on the subject, such as the front page of Le Point on January 26, 2017 «The day the Internet stops ... The new global cyberwar».

This issue paper by Afnic explores the possibility of such a general breakdown. Let's say right away, the conclusion will be nuanced: one cannot rule out the possibility of such a breakdown, but the scenario does not seem likely. That does not mean that the resistance of the Internet is sufficient, nor that we can rest on our laurels.

/// IS THE GLASS HALF FULL OR HALF EMPTY?

Answering the question is difficult because the answer will necessarily have to be nuanced, and be full of uncertainties. It is fairly easy to predict the number of road accidents that will occur next year.



Experience (alas) and the statistical law of large numbers leave only a certain margin of error. But exceptional events, such as a hypothetical total or almost total failure of the Internet, which has never happened, are obviously much harder to predict.

The pessimists will say that breakdowns and attacks are frequent, and have serious consequences. And they will cite examples such as ransomware blocking hospitals, malicious software preventing Rafale fighters from taking off, a denial of service attack preventing access to a popular site... And they will be indignant that a State, a small group of delinquents, or even a single high school student in his or her garage, can block such essential services.

Optimists will notice that none of these breakdowns or attacks have stopped the Internet, or even a significant portion of it. No matter how inconvenient the consequences for users of these particular services were, the Internet has continued to function. And the consequences were generally of short duration, a few hours at the most. We are far from the predicted «cyberwar».

This apparent opposition of points of view between optimists and pessimists can be summarized by the well-known quote of Pierre Col, «*the Internet is locally vulnerable and globally robust*». It is very easy (too easy, and that must be remedied) to cause limited failures for some time but much more difficult to do so on the scale of the Internet for a long time.

/// BUT WHAT EXACTLY IS THE INTERNET?

One of the reasons why discussions about the resistance of the Internet are difficult is that many people only know the Internet that they see on their screens. Hence the sensational title of the New York Times which announced during the attack against Dyn that «half the Internet has been broken». But the Internet continued to work perfectly well during the attack, even though several well-known sites were affected.

It is therefore important to remember that the Internet hosts a wide range of different services, and is not limited to half a dozen websites. Companies exchange data, scientific researchers copy large files, email and instant messaging services continue to work, even if Facebook is down.



Routers, the true heart of the Internet

When we talk about the Internet, we mainly think of the web pages of the best-known organizations, such as Google or Amazon. But the real infrastructure of the Internet is the hundreds of millions of kilometers of cable that connect the computers to each other, via routers, the active devices that point the messages in the right direction. There are many routers in the core, hundreds of thousands of machines, but they are produced by a small number of manufacturers (such as Huawei, Cisco or Juniper) and a failure or security hole affecting a whole range could have serious consequences. Here again, diversity is crucial for the good health of the Internet.

The world of routers is also that of the BGP (Border Gateway Protocol), which is not very secure (and, as with the DNS, the known security solutions are little deployed). Deliberate attacks, or accidents, such as the one committed by Google on August 25, 2017 and

which cut off part of the Internet especially in Japan, are of concern.

Up to now, cooperation between network operators has always allowed them to quickly mitigate the effects and then resolve these incidents.

The DNS, an essential and often forgotten link of the infrastructure

If cables, routers, and their BGP protocol form the core of the Internet, the Domain Name System (DNS) is an indispensable infrastructure. Without the DNS, there's virtually no Internet. (And, if you're something of a technician, do not say «Ah, but you can type the IP address to connect». With many web servers, it will not work - several servers on the same IP address - or will work badly - HTML pages that load code or style sheets, via URLs and domain names). The crucial nature of the DNS is highlighted during breakdowns such as that of Bouygues in April 2015 or the problem at Orange in October 2016, which black-listed Wikipedia and Google by mistake.

There are two different kinds of DNS servers: **authoritative servers** are maintained by domain name registries (such as Afnic, which maintains the authoritative servers for the .fr TLD), and **resolvers**, which are maintained by Internet service providers, local IT services or by large foreign operators.

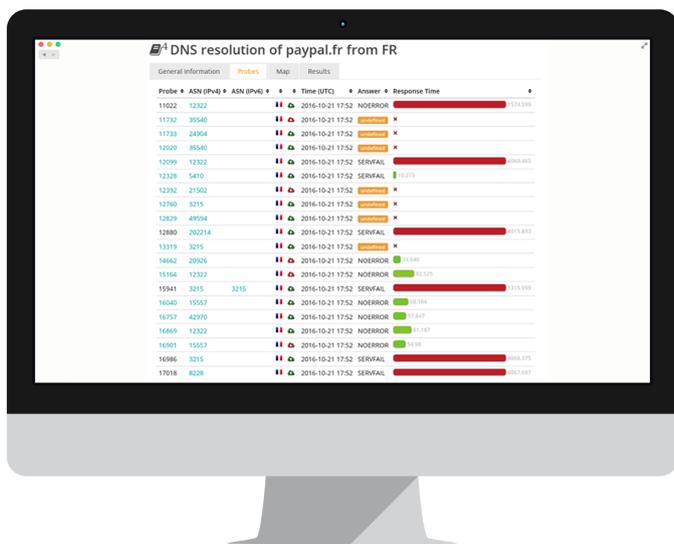
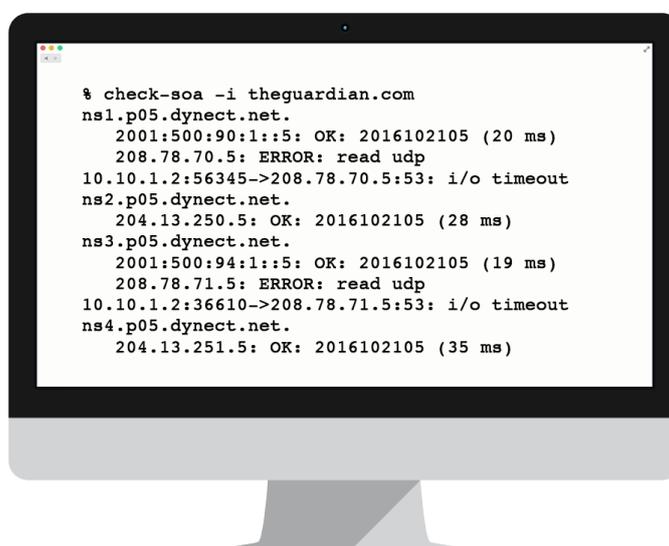
Both are crucial, and can be subject to attacks or breakdowns.

/// ATTACK AGAINST DYN IN 2016

This denial-of-service attack (an attack that aims to prevent a service from functioning, rather than take control of it) was one of the most spectacular in recent years. It hit the DNS host Dyn on October 21, 2016 in two phases. Each of the two phases lasted about two hours.

Note that, contrary to most media reports at the time, the majority of the known large websites that were affected by the attack were *not Dyn clients*. They were clients of Amazon Web Services, itself a client of Dyn (the AWS «end-points» in the eastern region of the United States are under the domain 'us-east-1.amazonaws.com' for which all the name servers were at Dyn). It resulted in a cascading outage, common on today's Web, where many external services are used just to display a page.

Here we can see, with a command-line measurement tool, for a press site that was a client of Dyn, and of Dyn alone, some of the name servers no longer responding. The attack consisted in sending huge amounts of traffic to the Dyn servers, which could no longer respond to all of the legitimate queries:

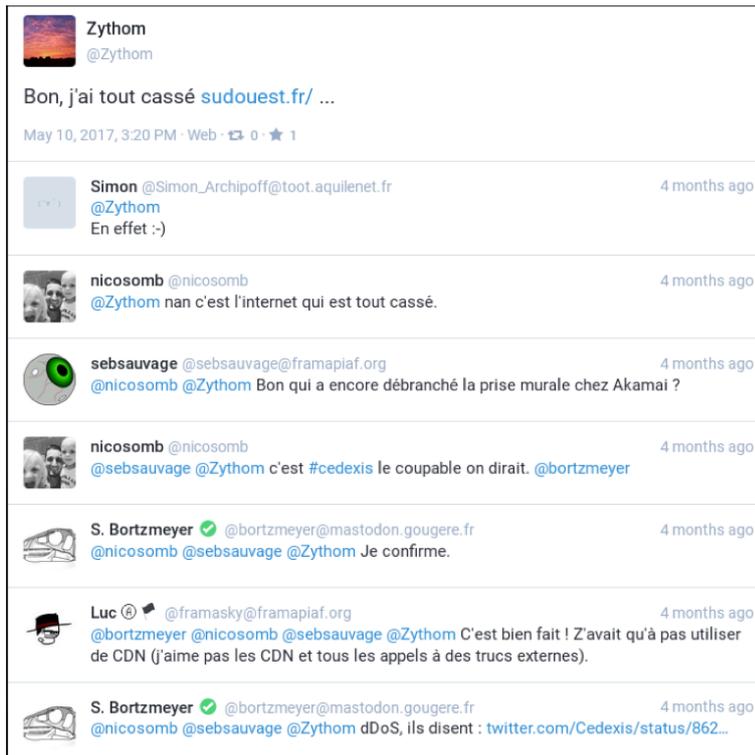


The attack seen by the RIPE Atlas probes. SERVFAIL = Server Failure. Undefined (in orange) is an absence of response from the resolver.

Other domains, which were hosted by Dyn and another vendor, had no visible problem.

/// THE ATTACK ON CEDEXIS AND ITS CONSEQUENCES

On May 10, 2017, the DNS host Cedexis was the victim of a denial of service attack lasting about two and a half hours. This host is used in particular by a large number of media, and the French press therefore was not very accessible on that particular day. This attack illustrates the crucial nature of the DNS, and the impression of «everything is broken» that a successful attack can give on a service widely used by the Web.



Social networks (here, Mastodon) are usually the best tool to learn that there is a breakdown!

Measured by the excellent network of RIPE Atlas probes, here is the effect on one hundred probes located in France. Half have failed in the DNS resolution (SERVFAIL = Server Failure):

```
% atlas-resolve -c FR -r 100 www.sudouest.fr
[195.154.181.181] : 10 occurrences
[ERROR: SERVFAIL] : 50 occurrences
[TIMEOUT(S)] : 33 occurrences
[37.187.142.180] : 5 occurrences
[62.210.93.5] : 2 occurrences
Test #8681136 done at 2017-05-10T13:23:15Z
```

Also read a post-mortem interview in French of the director of Cedexis : <https://www.nextinpact.com/news/104281-retour-avec-cedexis-sur-attaque-ddos-qui-a-rendu-partie-presse-inaccessible.htm>.

/// IMPROVING RESILIENCE

In fact, seriously wondering whether the Internet can be totally broken or not is a purely theoretical issue. On the one hand, it is very difficult to give a reliable answer to the question. On the other hand, it is more useful to ask what can be done to improve the resistance of the Internet.

For example, today there is too much centralization in some services. When Facebook is down, many users complain to their IT department that «the Internet is broken». And, indeed, for them, it is almost the same, since all their interactions are mediated (and recorded...) by Facebook.

More technically, if all of the DNS servers are hosted at A. and all of the sites at C., it can be seen that a breakdown of A. or C. will have far-reaching consequences. It is therefore crucial that Internet services, especially essential ones, are spread out over a large number of different providers.

These principles of redundancy and diversity must guide any design of Internet services. For example, redundancy means having multiple authoritative name-servers for a DNS zone, that do not share a common

point of failure (for example, they must not be in the same room). Another example of redundancy is that a country must be connected by a large number of very different physical links. Diversity means not putting all your eggs in the same basket. If all the Internet uses the same software as a DNS server, a security hole in the software has far-reaching consequences.

Note that the Internet Resilience Observatory in France (<https://www.afnic.fr/en/expertise/labs/achieved-projects/the-internet-resilience-observatory-in-france-2.html>) publishes an annual report, with a large number of indicators, such as the variety of network operators for a given DNS zone. (It also contains many excellent BGP indicators.)

Another measurement system, involving the entire community, is the deployment of RIPE Atlas probes (<https://atlas.ripe.net>), which allow numerous technical measurements from the most remote corners of the Internet.

Since it is difficult to predict breakdowns, and attacks even more so, human reactions are crucial to dealing with problems. This is why cooperation, consultation and coordination must be developed.

Finally, like any human endeavor, the Internet is not perfect and can fail. This risk must be incorporated into its security assessments, and systems must not be designed that produce dramatic consequences if the Internet has a specific defect at a specific time.

/// IN CONCLUSION...

Although we cannot provide a simple answer to the question «Can the Internet be broken?», on the other hand it is possible to work to **improve its resistance** (to withstand attacks) and its **resilience** (to recover after a crisis).

In addition, while breaking a part of the Internet for a limited time remains too easy, and justifies greater security efforts, fortunately for us, breaking the entire Internet for a long time is not within the reach of your average attacker.



USEFUL INFORMATION

To contact Afnic



Afnic
Immeuble Le Stephenson
1, rue Stephenson
78180 Montigny-Le-Bretonneux
France
www.afnic.fr



Tél. : +33(0)1 39 30 83 00



@AFNIC



support@afnic.fr



mastodon.social/@afnic



afnic.fr

About Afnic :

Afnic (the French Network Information Centre) comprises public and private stakeholders, including government authorities, users, and Internet service providers (Registrars). It is a non-profit organisation.

Afnic is the French Registry for the .fr (France), .re (Reunion Island), .yt (Mayotte), .wf (Wallis and Futuna), .tf (French Southern Territories), .pm (Saint-Pierre and Miquelon).

Afnic is also positioned as a provider of technical solutions and services for registries and registrars.

afnic