The .nlyst

INTERNET GOVERNANCE
An introduction

Historically, things such as telephone and postal services and energy supply were seen as the government's responsibility. Nowadays, however, they are largely privatised, although strictly regulated and supervised. By contrast, the internet has become a global phenomenon without government involvement. No one has overall control of this rather loosely connected network of computers. And governments have little say at all in how it is run. They aren't represented on the body that defines the technical standards (IETF) and the DNS is administered by a private organisation (ICANN).

Many people argue that it is precisely because of the absence of government interference that the internet has been so successful. In 1996, for example, John Perry Barlow, 'cyberspace activist' and co-founder of the Electronic Frontier Foundation published his 'Declaration of Independence of Cyberspace': an impassioned appeal to all governments to leave the internet alone. Although governmental involvement has since increased, much that happens on the internet and within organizations that make it work, is not subject to any form of specific government regulations. Of course it is subject to many national and international law. In many areas, there is debate as to whether and how governments should have a role, and what parts other groups such as the business community and users should play. The name given to this field as a whole is internet governance.

Broad concept
'Internet governance' is a very broad concept. It covers all sorts of topics, from access, openness, critical resources and the exclusion of child pornography to the improvement of internet access for people with impaired vision. These subjects are debated in a variety of forums and go by various names. The Dutch parliament's ongoing discussions on net neutrality come under the heading of internet governance, for example. In other words, internet governance isn't a tightly defined concept. Nevertheless, it does have a formal definition. At the World Summit on the Information Society (WSIS) in Tunis in 2005, a working group settled on the following definition:

Internet governance is the development and application by governments, the private sector and civil society, in their respective roles, of shared principles, norms, rules, decision-making procedures, and programmes that shape the evolution and use of the Internet.

Creation of the Internet Governance Forum
Another outcome of the WSIS in Tunis was the creation of the Internet Governance Forum (IGF). The IGF is a platform for the discussion of internet governance issues at the global level. Based on the multistakeholder model, the IGF does not make formal resolutions. The intention is that governments, academics, business people, community groups and others ➔

SIDN

Foreword

The sixth annual meeting of the Internet Governance Forum takes place in Nairobi between 27 and 30 September. The IGF is the global discussion forum for all manner of internet policy questions. Governments, businesses and representative organisations from all around the world attend IGF meetings to exchange ideas about issues such as access, privacy, security and the digital divide between developed and developing economies. Is it best to regulate or trust people to do the right thing? Which is preferable: national or global strategies? SIDN is one of the entities that have been active in the IGF since it was created.

SIDN is determined to play a part in debating internet governance issues. Primarily because, as a registry, we help to look after one of the foundation stones of the internet; the DNS is a critical resource, and therefore at the heart of the debate. Naturally, we want to communicate our views and expertise and help to shape international policy. By doing so, we hope to uphold the interests of the .nl domain and Dutch internet users.

Furthermore, 'noblesse oblige': the Netherlands consistently features at or near the top of internet league tables and the .nl domain is one of the biggest and most secure in the world. Because of its position and reputation, the Netherlands can influence the development of the internet for the better. And participating in IGF activities is one way of doing that. Finally, if big players like the Netherlands don't back the IGF energetically, the whole undertaking, with its unique multi-stakeholder structure, is bound to fail. In all probability, failure of the IGF would result in global discussion and decision-making on internet governance issues being taken over by governments and moved behind the closed doors of the United Nations. Such developments are likely to be particularly welcome to those states that want more control over what happens on the internet and over views that their citizens express there. It is vital for the continued development of the internet as we know it that the forces pulling in that direction are counterbalanced.

Because, although decision-making within the IGF is complex and slow, it remains the best option we have just now. We must not allow the future of the internet to be decided by closed inter-governmental processes within the walls of the UN.
The Netherlands will be sending a large delegation to Nairobi for this year's IGF. The Dutch Ministry of Economic Affairs, Agriculture & Innovation, ECP-ECN and SIDN have spent several months preparing for the meeting. The preparatory activities have included gathering input at a national forum, the NLIGF. The NLIGF is just one of the ways we collaborate with the Dutch government, one of the key stakeholders in our national consensus-based strategy of self-regulation.

Many of the discussions that take place at IGF meetings are abstract and policy-focused. And few yield tangible short-term results. Fortunately, here in the Netherlands, initiatives are constantly being taken that contribute directly and materially to the openness, diversity, accessibility, security and reliability of the internet. The best of those initiatives will again be recognised this year with SIDN Internet Awards. Entries for the awards are open until 5 October. More information is available at www.sidn.nl/awards.

Roelof Meijer
CEO, SIDN

An old chestnut: control of the DNS

One of the longest-running and most significant debates in the field of internet governance concerns the domain name system (DNS). The DNS, which makes it possible to find information on the web, is a hierarchical system. Consequently, a lot of its functionality depends on what happens at the top of the system (the 'root'). Whoever controls the root controls the system as a whole. And, because the internet started in the USA, control of the root has traditionally been in US government hands. Historically, that makes perfect sense: the internet is, after all, an American 'invention'. But, as the internet has become more international, some countries have become unhappy with the situation. Most western nations accept the US role, as long as the DNS is managed in an open, transparent and non-discriminatory way, and as long as policy is led by the interests of the internet community as a whole. However, countries such as Russia, China and Iran find it unacceptable that America should have control over a system that is so important for their economies. Theoretically, the US could at any point remove .ru, .cn or .ir from the root, making all the domain names within those zones unreachable or largely unreachable. The countries that are uncomfortable with America's power over the internet, generally supported by the world's developing nations, want to see control of the root switched to the United Nations and are threatening to develop their own DNS structure. So far, the US and its western allies have been able to resist the calls for change, however.

should be able to debate important issues in an open way, without the pressure of having to decide what should be done. Stakeholders therefore have the opportunity to understand each other's circumstances and thinking, and to work together to develop approaches that will have general support. Both the multistakeholder model and the non-conclusive nature of proceedings have often been questioned, however. There is a school of thought that an organisation that can't decide anything isn't really very useful. That par-

ticular point is likely to be debated for some time to come. On the other hand, many - among whom SIDN - feel that the IGF dialogue lead to broader and better understanding of important issues and thereby improve the quality of discussions taken else where.

Annual meeting

The IGF involves an annual gathering, lasting about a week. The first was in Athens in 2006, since which there have been meetings in Rio de Janeiro, Hyderabad, Sharm El Sheikh and Vilnius. This year's IGF takes place between 27 and 30 September, in Nairobi, Kenya. The last gathering attracted 2,700 people from 107 countries. A further 1,300 or so participated in proceedings via the internet. The programme of an IGF is very varied. It is compiled by the Multistakeholder Advisory Group (MAG), which, such its name suggests, is made up of people from all sorts of backgrounds. For each gathering, a number of central themes are nominated and stakeholders are then invited to suggest workshops relating to the themes.

Working groups during the IGF

Within the IGF, an important role is played by Dynamic Coalitions: working groups devoted to particular topics. Generally speaking, anyone with an interest in the relevant topic can join a Dynamic Coalition. There are coalitions for open standards, internet rights, press freedom and fighting child pornography. And the breadth of the internet governance concept is underlined by the existence of coalitions with names such as 'Internet and Climate Change', 'Gender and Internet Governance' and 'La Diversité Linguistique'.

Local and regional groups

Over the years since the IGF was created, local internet governance forums have sprung up in many countries. These groups exist partly to prepare topics for debate at the IGF, and partly to enable the discussion of local issues. They include Europe's regional governance forum Eurodig and the NLIGF here in the Netherlands. The latter forum was set up by the Ministry of Economic Affairs, Agriculture and Innovation,

ECP-EPN and SIDN. Its founders hope to involve as many Dutch stakeholders as possible in the discussion of national and international internet governance issues. The thinking behind the NLIGF is that wide involvement in the discussion of such issues will lead to better strategies. In line with that principle, the NLIGF organises meetings devoted to governance themes and participation in the organisation is encouraged. In the run-up to the IGF in Kenya, the NLIGF organised a meeting attended by a wide range of stakeholders, under the title 'The internet as a catalyst for change'. The day before, there was a Students' IGF, at which net neutrality, (il)legal downloading and the right to be forgotten were among the topics debated.

The future

It is hard to predict how internet governance will develop. Some of the governance issues currently in the spotlight are discussed by academic Michel van Eeten and SIDN CEO Roelof Meijer on this and the next three pages. What will be occupying minds a few years down the line, no one can say. The one thing that's certain is that, for a while to come, the IGF will be the platform on which the issues of the day are debated.

At the end of 2010, the UN extended the IGF's mandate for a further five years. It is possible, however, that there will be changes in the way the IGF operates: in 2010, a working group was created to explore possible improvements, but it has yet to come forward with any proposals.

THEORY V. PRACTICE
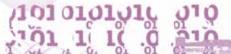## Professor Michel van Eeten and SIDN CEO Roelof Meijer talk about internet governance

Michel van Eeten and Roelof Meijer are both closely involved with questions of internet governance. One as a researcher, the other through day-to-day practice. Michel van Eeten is a Professor of Public Administration, blogger and writer, with a particular interest in the security of critical infrastructures, especially (in the last five years) internet security. Roelof Meijer is CEO at SIDN, one of the organizations that manages one of the internet 'critical resources': domain names. In this position he is dedicated to enhancing the security, accessibility and diversity of the internet and is involved with organisations such as the international Internet Governance Forum, ICANN and GOVCERT.

How did you come to be involved with internet governance?

RM: "My introduction to the subject was in 2005, not long after I joined SIDN. The UN held its World Summit on the Information Society, at which various aspects of internet were discussed, including internet governance. A lot of attention was given to the governance of critical recources on the inter-

net, such as domain names and IP addresses. And, of course, domain names are what SIDN is mainly concerned with, so inevitably I was drawn into those debates."

ME: "I got involved in this field in 2006. Internet governance was very much in the media spotlight at the time. What struck me was that the issues being discussed didn't actually seem to have much to do with internet governance. It was a long way from the operational reality of the internet. Only when it came to the DNS and ICANN were the issues really related to governance. So, for a long time, I was loath to use the term 'internet governance'. Then US internet governance expert Milton Mueller came to work in Delft, and we had some long discussions on the subject. Was it actually an appropriate term to use? What did it imply? I do now talk about 'internet governance' when explaining what I do, but I nevertheless published an article recently arguing that internet governance wasn't really about governance of the internet at all. In other words, I have a sort of love-hate relationship with the concept."

What is the hottest issue in internet governance right now?

ME: "The battle for control. A lot of what is currently happening under the banner of internet governance is actually people trying to understand or create internet governance, to enable control by governments or private entities. I have my doubts about many of the control mechanisms that are being developed, such as child pornography filters. I fear that moves to get a grip on the internet risk destroying much of what has made the internet so successful and innovative."

RM: "You could quite reasonably argue that there's actually no such thing as internet governance. There is no overall governance structure, just a huge range of organisations and less formal structures that all play a part in keeping the internet working and in facilitating its continued development. Each of them has its own role and its own form.
For me, the hottest issue is the striking absence of any overarching structure. Don't get me wrong: I'm not suggesting that we ought to have such a structure. I'd say that it's precisely because we haven't had one that the internet has been such a success. But it's a hot issue, because it inevitably leads to governments seeking to gain more control over what happens on the internet, sometimes with laudable motives, such

as protecting users, and sometimes with sinister motives, such as curbing freedom of expression. If the internet were under unilateral, centralised government control, there would be a real danger of losing the innovation and openness that has made it what it is. It may sound rather defensive, but one could almost say that the focus in internet governance should be on retaining all the good features of the internet and improving the things that can usefully be improved."

A recent UN report described cutting off the internet as a human rights violation. Is internet access a human right?

ME: "The UN criticised France and the UK for introducing laws that allow people to be excluded from the internet for illegal downloading of copyright-protected material. It is a punishment that in no way fits the crime. It's like banning someone from speaking if they are convicted of slander! So I have a lot of sympathy for the UN's view that internet access is something that should be withdrawn only in extreme cases. However, I think that describing it as a human right is going a bit far. Is driving a car a human right?"

RM: "I agree. Besides, it just isn't practical to try and make internet access a human right. Electricity isn't a human right, and without electricity you can't have internet access. Having a computer isn't a human right either. It's an overreaction to legislators' attempts to get a grip on the internet. The French were originally intending to allow for internet access to be cut off without the matter even going to court. That is really seriously devaluing internet access. However, if we really think internet access is important, we shouldn't be focusing on the few hundred thousand people who might theoretically be cut off for stepping out of line, but on the four billion people that don't yet have internet access at all. The digital divide, as it's called, is a much bigger problem. Not just morally, but pragmatically. In the Netherlands, you are at a tremendous disadvantage if you can't participate in the digital world. The same applies at the global level: there are entire countries that are being cut adrift."

ME: "My main focus is internet security. The digital divide is more of a peripheral issue in that field. Security issues can hit emerging economies harder. Nevertheless I take your point. ⇒

The question of how we can bridge the digital divide between countries is more tangible and more concerned with the future. There are enormous opportunities there."

Why doesn't a topic as important as the digital divide receive more attention?

ME: "I think that it has a lot to do with the lobbying power of big business. We've allowed ourselves to be held to ransom by copyright owners; by industries that have grown rich on the back of the historical accident that for forty years the only way to obtain sounds and images was to go out and buy physical media. Now these industries are behaving as if the survival of our culture depended solely on them."

RM: "It gets attention. But the people concerned are not best positioned to get their voices heard. On the contrary as an example the music lobby is certainly very strong. They are very good at getting their message across, at making sure everyone knows about the problems they face. And in addition, there are no quick and easy solutions to the digital divide and that tends to scare people off."

ME: "Another example is the battle against child pornography. When I first attended an IGF meeting, in Hyderabad in 2008, I attended various sessions on internet security. I was really surprised to discover that nearly all of them were in fact about child porn. Now, child porn may be very important in the context of crime detection and prevention, but it isn't a technical security issue. The preoccupation with this subject has the effect of displacing other, more relevant topics from the agenda."

RM: "The energy that goes into fighting child pornography is partly a reflection of the fact that it's something everyone can agree about. No one questions that it should be regarded as a crime. By contrast, there are people who argue that the copyright laws are unjust, for example. In the offline world there's no debate: breach of copyright is a crime. But as soon as the internet is involved, the debate goes in a different direction. There are suddenly groups calling for the law to be changed."

How should we protect children on the internet?

RM: "The obvious answer is: in exactly the same way as in the offline world. The government has a role to play, and so do information providers and parents. However, the various groups do need to work together and in some ways things are more challenging than in the offline world. Because, on line, you can't see the person you are dealing with. In a playground, you know whether your kids' playmates really are children. And a shop selling cigarettes can ask for ID. On line it's not so easy. As a result, in the Netherlands there is an ongoing discussion whether we shouldn't have an ID system for the internet. Then you could prevent minors visiting adult sites and adults pretending to be children."

ME: "There is absolutely no evidence that the internet makes child abuse easier to commit or harder to tackle than it is off line. Most abuse takes place off line, in places where children and adults are together. The mistaken belief that the internet is a hotbed for this kind of thing legitimises disproportionate control measures. I think that distorted perceptions of risk also play a part: the idea that things might be happening under our noses without us knowing is unsettling. On top of that, the internet is new; we have little experience to shape our perceptions. Research shows that, if people don't know how much risk a medium entails, they systematically overestimate it. I find it hard to envisage the consequences of going down the ID route, but the idea of it makes me uneasy."

RM: "I'm certainly not in favour of compulsory identification. But the use of ID isn't so much about preventing abuse as controlling access to content. A child can't walk into the local shop and walk out with a certificate-18 film, but at present we have no way of preventing the equivalent happening on line."

ME: "As the father of two young girls, I understand why people want tighter controls. There are sites that I'd rather my children didn't see. But I consider it primarily my responsibility, as a parent, to prevent that. You can't expect other people to do everything for you. Parents are still getting used to this new role, but gradually I think more and more basic guidelines are becoming established. Things like having the family computer in the living room, so that you can see what your children are getting up to on line. Or using a child-friendly browser. We have the Mybee browser on our PC, which I think is a really good solution."

Is tackling internet criminality the government's job, or is self-regulation the answer?

Roelof Meijer

SIDN's CEO since 2005. Before joining SIDN he was Managing Director at PTC+, an international training organization. Earlier he worked as engineer, project coordinator, technical consultant and government advisor for an engineering company and later the Dutch Ministry of Foreign Affairs in Zambia and Burkina Faso respectively. Meijer holds a master's degree in Engineering from Wageningen University.

ME: "I'm often asked the same question in The Hague and Brussels. In a nutshell, my response is: the government needs to enforce self-regulation. For the most part, you can leave things to the service providers. In fact, you should leave things to the industry wherever possible. However, you need to keep an eye on what they are doing. Not with a view to interfering with the nuts and bolts of how the industry regulates itself, but with a view to monitoring the effectiveness of the measures put in place. I'm a big advocate of ratings for things such as the providers' performance on security. Consumers say that security is important to them, but they have no way of knowing who provides the most security. The research we have conducted has highlighted some major differences.

A system of ratings would reward good service providers. Provided you have the incentive structures in place, self-regulation is very reliable. However, the detection and prosecution of crime are obviously jobs for the state. And there is no reason why crime committed via the internet should be any different to other crime. However, there's only so much you can do. The tools are not scalable, for example: every case requires just as much input. If you put in twice as much money, you don't suddenly get four times the effect. You can never devote the resources to stamp it out."

RM: "I agree. However, there are a few things you have to beware of. Sometimes, self-regulation means no regulation. Market players then tend to become passive and expect the government to do something about on line crime. On the other hand there have been cases where people have gone too far. For example, the governmentals requirement to provide traffic data.

It is a command opinion that it serves little purpose and means a lot of extra trouble and expense for internet service providers. Fortunately, there is an increasing realisation in government circles that you can't plug every gap with laws and regulations and that introducing legislation doesn't necessarily mean that a problem will disappear. Overall, I think the Netherlands has it about right: let the sector regulate itself and intervene only when things aren't working. Legislation should be kept in reserve, to focus everybody's mind."

With that, SIDN's CEO and Professor van Eeten concluded a discussion that ably demonstrated the breadth and current dynamism of the subject of internet governance. Those characteristics will undoubtedly be in evidence again at the IGF meeting scheduled for Nairobi, Kenya, where SIDN will of course be represented.

Michel van Eeten

Academic, blogger and writer. As well as working for the TU Delft as Professor of Public Administration, Michel van Eeten teaches at the Dutch School for Public Administration in The Hague. He has advised a variety of organisations and institutions, including the Ministry of Economic Affairs, the International Telecommunication Union and the OECD. In 2008, his pieces on Bijzinnen.com won van Eeten an award for the best written Dutch blog. His first novel Tegennatuur (literally 'Anti-Nature') was long-listed for the 2009 AKO Literature Prize.

LEARNING IN A MULTISTAKE-HOLDER ENVIRONMENT
Summer School on Internet Governance (SSIG)

In 2005, when the UN Working Group on Internet Governance (WGIG) presented its report to the UN World Summit on the Information Society, it highlighted a lack of opportunities to study internet governance. Academic WGIG members therefore prepared a plan for an independent Summer School on Internet Governance (SSIG). A European pilot project followed in 2007, in Meissen, Germany.

About 70 fellows from 30 countries applied for the 20 seats. EURO-SSIG became a great success. Applications are growing year by year and EURO-SSIG now accepts 30 fellows per course. More than 600 people applied in the last five years and around 150 fellows received the Meissen-SSIG Certificate. Anybody can apply for the EURO-SSIG who has a basic knowledge of internet governance and a bachelor's degree or equivalent experience. We prefer students who like working in an international, multistakeholder environment.

The one-week programme includes 60 hours of lectures, case presentations, panel discussions, interactive workshops and students' presentations. The curriculum combines lectures on internet governance history, theory, policy and security with practical presentations on technical issues like internet standardisation, management of critical resources, business problems and policy themes. In the evening, fellows make so-called "country presentations".

Along with lectures by academics such as William Drake, Avri Doria, Milton Mueller and Olga Cavalli, highlights of the 2011 EURO-SSIG were a lecture by ICANN Director Bertrand de la Chapelle, a business roundtable, moderated by Ayesha Hassan from ICC with IG experts from industry, and case presentations on IP addresses and domain names.

SSIG's slogan is "Learning in a Multistakeholder Environment". And participants do indeed represent the range of IG stakeholder groups from academia, business, the technical community, civil society and government, allowing fruitful interaction among fellows and faculty members.

Another SSIG slogan is "Teaching the Internet Governance Leaders of Tomorrow". Just five years after SSIG's start, several fellows and faculty members have secured leadership positions in ICANN, IGF and other bodies. At the ICANN meeting in Singapore, 20-plus former SSIG fellows and faculty members participated and now serve on the ICANN Board, GAC, ALAC, GNSO and ccNSO Council. Also in the IGF Multistakeholder Advisory Group (MAG), former SSIG fellows are now translating SSIG knowledge into action.

SSIG's success has been made possible by support from the internet community, particularly the ccTLD constituency. SIDN was one of the first ccTLDs to recognise the need to invest more in capacity building. Since 2008, SIDN has been a silver sponsor and funded fellows from developing countries. Other sponsors include RIPE NCC, DENIC, nic.at and NORID.

Inspired by EURO-SSIG's success, SOUTH-SSIG began in 2009. There have now been summer schools in Buenos Aires, Sao Paulo and Mexico City. Before the Sharm el Sheikh IGF, an ARAB-SSIG was organised with the Egyptian Telecommunication Regulatory Authority in 2009 in Cairo. There are also plans under discussion for SSIGs in Asia and Africa. The main organiser is Medienstadt Leipzig e.V, an ICANN-recognised At-large Structure.

Prof. Wolfgang Kleinwächter
University of Aarhus,
Chair of SSIG Faculty

ICANN Internet Corporation for Assigned Names and Numbers, **GAC** Governmental Advisory Committee
ALAC At-large Advisory Committee, **GNSO** Generic Names Supporting Organization, **ccNSO** Country Code Names
Supporting Organisation, **RIPE NCC** Réseaux IP Européens Network Coordination Centre, **DENIC** Deutsches Network
Information Center, **NORID** Norwegian registry for Internet domain names, **ICC** International Chamber of Commerce

Regulation at the periphery:
THE END-TO-END PRINCIPLE AND INTERNET FREEDOM

Ot van Daalen, director Bits of Freedom

The end-to-end principle has proven to be an important internet design principle. But it can be more than that: it can be a useful paradigm for the design of internet policy. Such an approach also promotes internet freedom, argues Ot van Daalen of Dutch digital rights movement Bits of Freedom.

The end-to-end principle implies designing a network so that application-specific functions are implemented at the periphery; network nodes merely transmit the information sent by peripheral applications. For example: computer A transmits a message to computer B. In a network not designed according to this principle, intermediary nodes analyse the message, determine the ultimate destination, and establish an application-specific connection between computer A and computer B. The message is subsequently transmitted to computer B.

On the other hand, in a network designed according to the end-to-end principle, computer A divides the message in packages, transmits those packages to the first node of the network, without regard to the application for which the package is intended, which transmits them to the next node, etc. The message is then reassembled at computer B.

Historically, the internet has been designed mainly on the end-to-end principle. Its architects recognised that they couldn't foresee how the internet would be used. This approach allowed all kinds of innovative applications to be developed and offered over the internet, without the need to upgrade the intermediary nodes. It made the internet flexible. But the end-to-end principle is not relevant only for internet design. It is also a useful paradigm for the design of internet policy. A cautious approach, preferring the enforcement of regulations at the periphery, enhances internet freedom.

By enforcing regulations at the periphery, collateral damage to communications freedom can be minimised. For example:

blocking access to an entire website containing unlawful material – enforcing regulations within the network – risks blocking legitimate material too. A more focused approach would be to remove the illegal material from the website itself – at the periphery – and leave the legal material intact. Collateral damage to privacy can also be minimised. Installing invasive surveillance technologies at internet exchanges – enforcing regulations within the network – means interception of enormous amounts of traffic between innocent internet users. Whereas intercepting the traffic from the connection of one suspect ensures that innocent users' traffic remains untapped.

Enforcing regulations at the source nodes has another benefit: it allows for a more focused approach to tackling the core problem. The mere blocking of access to websites distributing child abuse material does not stop the material's distribution or hit the perpetrators – it merely attempts to minimise the problem's symptoms. Far better would be to remove the images and prosecute the perpetrators, i.e. tackle the core problem.

The years ahead will no doubt see further internet policy proposals targeting copyright infringement, cybercrime and terrorism. When evaluating each proposal, we should first consider whether regulation is necessary at all. If it is, we need to explore whether enforcement at source is possible and think twice before implementing enforcement measures in the network itself. This allows for a focused approach to internet regulation while protecting internet freedom.

The.nlyst

.NL Analysed

TLD top 25 ranking Q2 2011

	TLD		Count Q2*	Growth	
1	.com	Generic	95,736,361	1.9%	=
2	.de	Germany	14,483,611	1.2%	=
3	.net	Generic	13,988,941	1.2%	=
4	.uk	United Kingdom	9,490,537	1.9%	=
5	.org	Generic	9,255,687	1.8%	=
6	.info	Generic	7,876,203	2.9%	=
7	.nl	Netherlands	4,513,620	3.3%	=
8	.cn	China	3,502,288	3.4%	=
9	.eu	European Union	3,346,401	-1.0%	=
10	.ru	Russia	3,331,219	2.5%	=
11	.br	Brasil	2,547,329	5.6%	=
12	.ar	Argentina	2,339,908	2.6%	=
13	.it	Italy	2,210,562	2.9%	=

	TLD		Count Q2*	Growth	
14	.pl	Poland	2,137,520	3.1%	↑
15	.au	Australia	2,129,801	4.9%	↑
16	.biz	Generic	2,104,280	1.0%	↓
17	.fr	France	2,054,746	3.5%	=
18	.us	Canada	1,715,279	3.7%	↑
19	.ca	United States	1,680,912	0.1%	↓
20	.ch	Switzerland	1,594,382	2.0%	=
21	.es	Spain	1,354,137	4.5%	=
22	.jp	Japan	1,220,197	0.8%	=
23	.be	Belgium	1,156,953	2.6%	=
24	.dk	Denmark	1,128,265	1.2%	=
25	.se	Sweden	1,106,412	2.1%	↑
	*By June 30, 2011				

The growth of the top 25 TLDs slowed by 11 per cent in the second quarter of 2011. The net number of domain names added fell back from 4.2 million in Q1 to 3.7 million in Q2. Overall TLD growth followed a similar pattern, being 13 per cent down on the previous quarter.
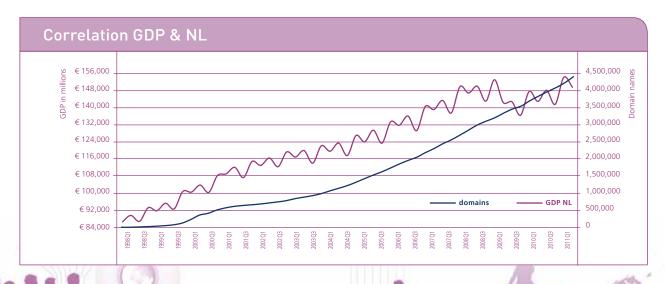
Amongst the top 25 TLDs, there were some interesting developments. China's ccTLD started growing again, enabling it to stay ahead of .eu. By contrast, the European TLD had a difficult quarter, slipping into negative growth; .eu now looks almost certain to be overtaken by .ru. As anticipated, .biz slipped a couple of places in the league table. Meanwhile, .ca has overtaken .us, underlining the success of the registry's promotional activities. There is also a new name in the top 25, after .se displaced .kr, as widely forecast.

.NL correlation

From research that SIDN has carried out amongst former registrants and former registrars, it is clear that the economic climate has a strong influence on growth in the number of domain names. A publication by SEDO, the domain name trading platform, backs up SIDN's findings. SEDO has recently launched a Price Index for Internet Domain Names (www.idnx.com), which shows that there is a correlation between the buoyancy of the NASDAQ and the selling prices of domain names. In the Netherlands too, a close correlation can be observed between economic indicators and domain name sales. In our case, there is a strong link between gross domestic product (GDP) and the number of .nl domain names, as this graph shows. In the graph, GDP (expressed in millions of euros) is plotted against the total number of .nl domain names. The correlation coefficient is 0.93, indicative of a close relationship.

[1] A value of +1 or -1 is indicative of a linear correlation, while 0 means no correlation at all.
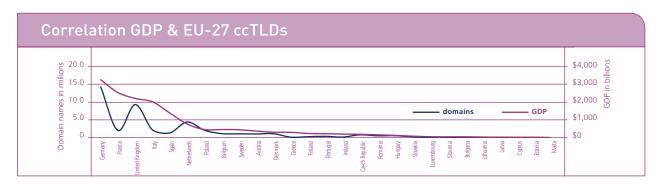

Correlation GDP & NL

.EU correlation

Looking at the 27 EU member states, similar correlations can be seen between GDP and ccTLD domain name count, as shown in this graph. It is striking that France, Italy and Spain lag a long way behind the other European TLDs in terms of their size relative to the potential market. The overall correlation coefficient between ccTLD size and GDP is 0.82. However, if the three 'laggers' are excluded from the calculation, the correlation coefficient rises to 0.99. One critical factor

explains why France, Italy and Spain differ from other EU countries: adherence to a restrictive registration policy. To register a .fr or .es domain name, a business or private individual has to demonstrate significant ties with the relevant country. Until 2004, Italy applied rules limiting private individuals to a single .it domain name (although businesses could register as many as they liked). Furthermore, a .it domain can be registered only by a person or business living or based in an EU member state.

Correlation GDP & EU-27 ccTLDs
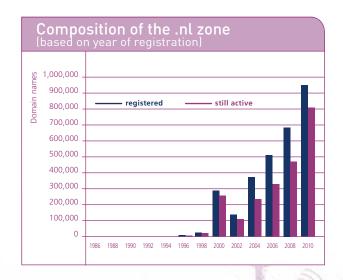
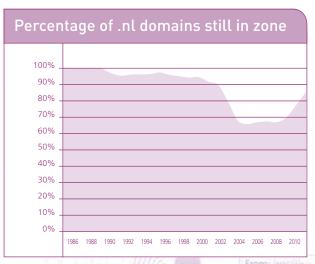**Breakdown of the .nl zone by registration date**

In 2011, the .nl domain celebrated its silver jubilee. A good time to consider how the .nl zone – all active .nl domain names – breaks down in terms of the names' registration dates. Registration date analysis is a useful way of highlighting developments in market dynamics. Nearly all the domain names registered during the dot-com bubble – from 1995 to 2000 – are still in the zone.

The liberalisation of .nl in 2003 – when it became possible for private individuals to register .nl domain names – and the rise of broadband internet access generated much more dynamic patterns of development. The number of registrations has grown almost exponentially since 2003. Increased dynamism

is clearly reflected in the increasing gap between the number of domain names that have ever been registered and the number that remain active. The gap is the result of much higher rates of cancellation since 2003. Nevertheless, about 77 per cent of all the .nl domain names ever registered are still in the zone.

This graph shows what proportion of the domain names registered in a given year remain in the zone today. Higher cancellation levels since 2003 are reflected in the declining percentage of domain names that remain active. From the average age of a domain name – four years – it is apparent that the proportion of domain names that remain active has started to rise again since 2008.

Composition of the .nl zone
(based on year of registration)

Percentage of .nl domains still in zone

Did you know...?

… that this month, as part of the celebrations to mark the .nl domain's silver jubilee, SIDN and PwC are organising the great National Internet Survey? The intention is to gather information about the economic, social and personal significance of the internet to the Netherlands, now and in the future. The findings will be discussed at the Silver Jubilee Congress on 10 November 2011, at TAETS in Zaandam, Holland. At the congress, national and international experts will also be presenting their ideas on important, topical internet-related themes. You can get your voice heard by taking part in the National Internet Survey. Simply go to www.denationaleinternetenquete.nl and complete the questionnaire before 30 September 2011.

de Nationale Internetenquête

Suggestions

If there is a topic that you think we should be covering in The.nlyst, please send your suggestions to: communicatie@sidn.nl.

Event calender

SIDN frequently sends representatives to national and international congresses. We undertake these activities in our capacity as the registry for the .nl domain and the Dutch ENUM zone. In doing so, we seek to represent the Dutch internet community and our registrars. In addition, we ourselves organize regular gatherings for our registrars.

In the coming months, SIDN is represented at the following conferences:

Date	Event	Place
27-09 to 30-09	IGF KENYA 2011	Nairobi, Kenya
06-10 to 07-10	46th CENTR GA	Brussels, Belgium
23-10 to 28-10	42nd ICANN meeting	Dakar, Senegal
30-10	25th CENTR Tech	Vienna, Austria
31-10 to 04-11	RIPE 63	Vienna, Austria
10-11	25 years of .nl congres	Zaandam, The Netherlands
13-11 to 18-11	82nd IETF	Tai Pei, Taiwan
15-11 to 16-11	Govcert Symposium	Rotterdam, The Netherlands

The .nlyst

In the next issue:

→ who are the .nl registrars?

From: isoc
To: info@sidn.nl
Cc:

MIX
Papier van verantwoorde herkomst
FSC® C020192
FSC
www.fsc.org