## CONTENT

<table>
<thead>
<tr>
<th>Contributors to this Issue</th>
<th>4</th>
</tr>
</thead>
<tbody>
<tr>
<td>Editorial</td>
<td>5</td>
</tr>
<tr>
<td>Team</td>
<td>5</td>
</tr>
<tr>
<td><strong>Who Rules the Internet?</strong></td>
<td>6</td>
</tr>
<tr>
<td>Online Reputation And Internet Abuse – An Interconnected Problem?</td>
<td>9</td>
</tr>
<tr>
<td>Trust, Global Cooperation and Self-Regulation – A very, very fast approach to cope with illegal content</td>
<td>11</td>
</tr>
<tr>
<td>Healthy Domains Initiative: Healthy Practice Areas for Domain Registries and Registrars</td>
<td>14</td>
</tr>
<tr>
<td>Internet Governance: Bringing Order to the “Digital Wild West” from the Bottom Up</td>
<td>16</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>The Why, How, and Who of Internet Governance</th>
<th>18</th>
</tr>
</thead>
<tbody>
<tr>
<td>A Quiet Global Revolution</td>
<td>22</td>
</tr>
<tr>
<td>Access, Human Rights, and Getting the Next Billion Online – The IGF as a Global Multi-Stakeholder Platform</td>
<td>26</td>
</tr>
</tbody>
</table>
A Day in the Life of a Man with a Key to the Internet 28

DNS – Claiming and Protecting Virtual NameSpace 34
The Domain Name System –
Making a Company Website Findable 37
Mapping Virtual Space to the Geographical Environment – The Growth and Management of New geoTLDs 40

Why Self-Regulation Runs in the Country’s DNA 42
GmbH: Exclusiveness Increases Value 43

Publication Details 46
CONTRIBUTORS TO THIS ISSUE

Wido Potters, Board Member of the AbuseIO Foundation, Manager Support & Sales at BIT BV

Alexandra Koch-Skiba, Head of eco Complaints Office, eco – Association of the Internet Industry

Mason Cole, Chair of the DNA Healthy Domains Initiative Committee

Vittorio Bertola, Research & Innovation Engineer, Open-Xchange

Thomas Rickert, Attorney at Law & Owner, Rickert Rechtsanwaltsgesellschaft mbH

Prof. Michael Rotert, Chairman of the Board, eco – Association of the Internet Industry

Olaf Kolkman, Chief Internet Technology Officer, Internet Society

Sven-Holger Wabnitz, Visionary & Advisor

Dirk Krischenowski, Founder/CEO, dotBERLIN GmbH & Co. KG

Marco Hoffmann, Head of Domain Services and Product Management, InterNetX

Please note: The opinions expressed in Industry Insights published by dotmagazine are the author’s own and do not reflect the view of the publisher, eco – Association of the Internet Industry.
Klaus Landefeld, Member of the Board at the eco Association, on ensuring the survival of cyberspace as we know it – by avoiding nationalistic tendencies in global governance

Politics, having failed to establish even the bare minimum of cross-national agreements, and being faced with digitalization in all aspects of modern life, is developing a certain disregard towards the international aspects of the net.

Navigating the thin line of lawful operation on a global scale is becoming close to impossible for a multinational service

Irrespective of the world region, be it North America, Europe, Russia, or China, national regulations and requirements are being toughened to a point where navigating the thin line of lawful operation on a global scale is becoming close to impossible for a multinational service.

When one country’s data retention is another’s breach of privacy, how can service providers operate an international platform?

When one country’s requirement for data retention is another country’s breach of privacy; one country’s prohibited hate speech, another country’s protected freedom of speech – how are service providers expected to operate an international platform? How does one resolve conflicting cultural differences and expectations?

Where are the boundaries of national sovereignty in the borderless Internet?

And this is just the tip of the iceberg: With more and more countries establishing laws to enforce national rulings on an international level, even declaring the whole of “cyberspace” as a legal ground of operation for law enforcement with no national boundaries whatsoever – where does this leave us? Where are the boundaries of national sovereignty, and how far is the reach of national law?

As difficult as it may be in the new world order of “my nation first” – it is imperative to quickly resolve these conflicts, to find a common ground for internationally acceptable rules and regulations in order to ensure the survival of cyberspace as we know it.

On that note, welcome to the latest issue of dotmagazine, “Who rules the Internet?” – where we look into the mechanisms of global governance and self-regulation that are helping to keep cyberspace healthy, and we offer insight into the Domain Name System – how the telephone book of the Internet connects us all.

Klaus Landefeld,
Board Member & Director for Infrastructure and Networks
eco – Association of the Internet Industry

Read the article online here: https://www.dotmagazine.online/issues/who-rules-the-internet/doteditorial-march-2017
Because the Internet is not a single infrastructure, it is easy to lose track of everybody involved in Internet Governance. Yet, nothing beats the multi-stakeholder approach.

An attempt to describe the Internet in one sentence: The Internet is a cross-national infrastructure of cables, routers, switches and servers that rely on multiple services, applications, standards and protocols that allow anyone to exchange data with anybody else, and it is impossible to say who runs or owns the Internet or even understand and agree upon everything necessary to keep it running – which doesn’t keep us from trying.

It is impossible to say who runs or owns the Internet or even understand and agree upon everything necessary to keep it running - which doesn’t keep us from trying

Keep us from trying? Who is “us,” exactly? It’s hard to say. Just like there is no single central Internet, but rather a variety of autonomous networks, there is no single central party governing the Internet. Instead, we have ICANN with IANA, IETF, IGF, W3C, and the ITU, to name just a few. For a longer list, visit Wikipedia (https://en.wikipedia.org/wiki/Internet_governance#Internet_bodies), but don’t count on that list being complete.

As for eco – Association of the Internet Industry: eco actively supports and participates in a number of international committees, such as the IGF, whose last meeting took place in Mexico in December. Michael Rotert, eco’s Chairman of the Board, was there to represent the Internet industry in discussions that ranged from multi-layered IT security connections to sustainable development and human rights in the digital age.

Multi-stakeholder approach

Conferences like these display the full diversity of Internet stakeholders and leave no doubt that fair and efficient Internet governance is not achieved by centralizing power, but rather by working on the multi-stakeholder approach. It won’t come easy, but we are making good progress.

“The open and self-regulating multi-stakeholder approach needs constant improvement and adjustment. Stronger cooperation is already taking place at all levels. The Internet
has become ubiquitous, and digitalization is advancing in all areas. For this to succeed, open discussions need to continue at all levels," Michael Rotert stated at the Mexico conference. (Read Michael Rotert on the work of the IGF in “Access, Human Rights and Getting the Next Billion Online”, this volume, pg. 26)

For more on the major players in Internet governance and the multi-stakeholder approach, see A Quiet Global Revolution, this volume, pg. 22 and The Why, How, and Who of Internet Governance, this volume, pg. 18.

**Nationalization of the Internet**

*Even basic principles such as openness, transparency, and neutrality are the subject of ongoing negotiations*

With stakeholders coming from all countries in the world and different political, social and industrial backgrounds, consensus is often hard to reach. Even basic principles such as openness, transparency, and neutrality are the subject of ongoing negotiations and, as can be expected, interpreted differently in different parts of the world. Germany and other European countries are no exception. Attempts to nationalize the Internet are frequent, and these come from politics, the industry, and also Internet users.

*...navigating the thin line of lawful operation on a global scale is becoming close to impossible for a multinational service*

Klaus Landefeld, eco Director of Infrastructure and Networks warns: "Irrespective of the world region, be it North America, Europe, Russia or China, national regulations and requirements are being toughened to a point where navigating the thin line of lawful operation on a global scale is becoming close to impossible for a multinational service. As difficult as it may be in the new world order of "my nation first" - it is imperative to quickly resolve these conflicts, to find a common ground for internationally acceptable rules and regulations in order to ensure the survival of cyberspace as we know it." (Read more from Klaus Landefeld in the doteditorial, this volume, pg 5).

**Self-regulation initiatives**

One very successful area of self-regulation is the Internet industry’s processes for dealing with illegal online content, through the complaints offices of the global INHOPE network, for example. "Self-regulation of the Internet is very important," according to Alexandra Koch-Skiba, Head of the eco Internet Complaints Office. “It is not only the basis of the eco Complaints Office [but even more] it is the approach of our members. Many years ago, they talked about the best way to fight illegal content, and one of the results was the founding of the eco Complaints Office, and we still stick to the self-regulatory approach. So it’s us who inform the providers, instead of governmental authorities. It is a very, very fast approach, and being fast when it comes to illegal content is one of the important things." (Read the interview with Alexandra Koch-Skiba, Trust, Global Cooperation and Self-Regulation – A very, very fast approach to cope with illegal content, this volume, pg. 11)

Another area where self-regulation has proven to be successful is in the area of security and abuse. According to Wido Potters, who established the free-to-use, open source network abuse support project AbuseIO, "Abuse is becoming increasingly problematic on the Internet. It consumes large amounts of resources and reduces the public trust in the online world. This negatively affects businesses worldwide, especially the Internet industry. For quite some time, Dutch Internet industry organizations have been warning the industry that if they do not solve the problem themselves, the politicians will solve it for them. It is likely that their solution will not benefit the industry." (Find more on AbuseIO in Online Reputation and Abuse – An Interconnected Problem? in this volume, pg. 9)

Another recent initiative is the Healthy Domains Initiative (HDI), established by the Domain Name Association, with its recommendation of “Healthy Practice Areas for Domain Registries and Registrars” (Read more about the HDI in this volume, page 14). According to Mason Cole, Vice-President of Donuts and Chair of the DNA Healthy Domains Initiative Committee “While HDI is designed primarily to advance the safe and beneficial evolution of the domain name system, its secondary goal is to demonstrate to Internet stakeholders the capability of industry operators to effectively self-regulate. HDI is not under the aegis of ICANN or any other regulator — it’s an industry-led program that operates independently, guided by the organizations that have the operational experience to help keep the namespace healthy."

**Openness and Transparency**

*If you want to implement better security methods, all companies have to support them. No ISP can do this alone*

Openness and transparency are also two principles held dear by supporters of open source solutions. Vittorio Bertola of
Open-Xchange believes that software-as-a-service solutions used by hosting, service providers and telecommunications should be based on open source. “As we make some fundamental free building blocks of the net, such as Dovecot and PowerDNS, and as we power the email, collaboration, and domain name resolution of many of the biggest ISPs around the world, we put some real effort into making our software open, secure, and free (as in free speech) as much as any company could,” says Bertola (Read more from Vittorio Bertola in Brining Order to the Digital Wild West from the Bottom Up, this volume, pg. 16). “Email security, in particular, is a field that can only advance by bottom-up cooperation. … If you want to implement better security methods, all companies have to support them. No ISP can do this alone, at least not if you still believe in the traditional principles of the Internet.”

We don’t ask ourselves, “who rules the Internet?” What we really want to know – “Is this thing safe?”

Privacy, integrity and trust – they may be among the most important goals we should set when we try to improve Internet governance. Because after all, when we turn on our Internet devices, we don’t ask ourselves, “who rules the Internet?” What we really want to know – “Is this thing safe?”

Mathias Röckel

The best way to get rid of illegal content

Illegal Internet content is not only damaging to the industry. It can also be very dangerous, especially when personal privacy is at stake. Of the many strategies suggested and tested, one sticks out as exceptionally successful: user integration combined with self-regulation.

How is it done?

1) Users encounter illegal content online, for instance, a racist statement in a forum, a disturbing image, or spam.

2) Users report that content to their respective Complaints Office, such as the eco Internet Complaints Office: https://international.eco.de/internet-complaints-office.html

3) The Complaints Office will then examine the content and take measures such as getting in touch with the content provider or the hosting provider and the appropriate law enforcement agency. The goal is to take the content offline.

Does it work?

In the second quarter of 2016, the German Complaints Office received reports of 175 cases of Child Sexual Abuse Material (CSAM) online, 42 % of which were hosted in Germany. 96 % of these cases were offline within one week. https://international.eco.de/wp-content/blogs.dir/2/files/internet-complaints-hotline-statistics.pdf

How about international cooperation?

The Internet crosses borders and so does the Complaints Office Community. More than 45 Complaints Offices from 40 countries are united under the umbrella of INHOPE – the International Association of Internet Hotlines (http://www.inhope.org/gns/home.aspx). Members collaborate with each other via INHOPE. As a result, complaints can be pursued in the land of origin.

Read the article online here: https://www.dotmagazine.online/issues/who-rules-the-internet/who-rules-the-internet
Handling abuse is one of the most tedious chores while running an ISP. It is not only boring, but is nearly always time consuming. This can result in abuse handling becoming extremely costly, as there is no monetary compensation for all the time spent on it. It is, however, beneficial for your customers and for the Internet. There are ways to help you in your fight against abuse in your network.

The solution is automation. eco-member BIT (https://www.bit.nl/) started the open source, 100% free-to-use project called AbuseIO (https://abuse.io/). AbuseIO is a self-hosted toolkit that anyone can use to receive, process, and correlate abuse reports, and send notifications to end users with specific information regarding the abuse case(s). It handles reports from Shadowserver, IP Echelon, SpamCop, Netcraft, and many others. AbuseIO’s purpose is to consolidate efforts by various companies and individuals and to automate and improve the abuse handling process. After the initial setup, it will reduce the time spent on abuse handling by an order of magnitude.

Abuse is becoming increasingly problematic on the Internet. It consumes large amounts of resources and reduces the public trust in the online world, negatively affecting businesses worldwide.

Screenshot: Botnet infection detected by AbuseIO
public trust in the online world. This negatively affects businesses worldwide, especially the Internet industry. This growing problem is attracting more and more attention from politicians. For quite some time, Dutch Internet industry organizations have been telling their members to take action against abuse. These organizations have been warning the industry that if they do not solve the problem themselves, the politicians will solve it for them. It is likely that their solution will not benefit the industry.

The Internet is becoming more aware of reputation and hosts with varying reputations are treated differently, for example in spam filtering, where complete networks are regularly blocked.

Besides the possibility of unbeneficial governmental measures against Internet companies and the reduced public trust, there are other reasons why Internet companies should minimize abuse on their networks. Abuse attracts abuse. A compromised host in your network will be targeted for several types of abuse and might become a victim of retaliation attacks. Abuse hurts reputation. The Internet is becoming more aware of reputation and hosts with varying reputations are treated differently. The best known example of this can be found in the field of spam filtering, where the blocking of complete networks regularly occurs. Furthermore, Internet companies should be aware that vulnerable hosts will lead to abusive hosts. Therefore, it is worthwhile to solve the problem early on by identifying vulnerable hosts before they become abusive.

A mid-size, well-known and respected hosting company in the Netherlands was shocked by the result of 30,000 abuse cases and vulnerabilities in their network when they started using AbuseIO. Within weeks, they reduced this to several hundred cases and vulnerabilities.

Since the ‘birth’ of AbuseIO a year and a half ago, dozens of Internet companies have started using the software. Many of them have told us that the amount of time spent on abuse handling has been slashed and most of them were unaware of the number of vulnerable and abusive hosts in their network. Once you start looking for abuse in your network, the problem usually turns out to be a lot bigger than expected. A mid-size, well-known, and respected hosting
company in the Netherlands was shocked by the result of 30,000 abuse cases and vulnerabilities in their network the moment they started using AbuseIO. Within weeks, they reduced this to several hundred cases and vulnerabilities. That is the power of automation.

It also demonstrates the power of informing your customers. The majority of your customers are not consciously facilitating abuse. They are unaware of the problem(s) on their host(s) and appreciate being informed. AbuseIO informs the person/organization running the problematic host and it provides tools to resolve the issue(s).

The next step AbuseIO will take in the fight against abuse is to provide tools to send out abuse complaints. There are many organizations that hold information on vulnerable and abusive hosts on the Internet, but they are without the means with which to reach out to the operators of these hosts. We believe that the only way to begin to solve the Internet abuse problems is in cooperation and the sharing of information.

TRUST, GLOBAL COOPERATION AND SELF-REGULATION – A VERY, VERY FAST APPROACH TO COPE WITH ILLEGAL CONTENT

For all the boundless potential and opportunities that the Internet offers, there is also the dark side to the web. Given the borderless nature of the Internet, cross-border, transnational cooperation is vital to keep user data secure, but also to keep users themselves safe. The ongoing fight against illegal content in the Internet requires just such cooperation between the public, content analysts, industry players like Internet service providers and content delivery networks, and law enforcement. While complaints hotlines around the world deal with a whole range of different types of illegal content, probably their most important, and most personally challenging work is dealing with images of child sexual abuse. dotmagazine spoke to Alexandra Koch-Skiba, Head of the eco Complaints Office, on her team’s valuable contribution to the fight against such material.

DOTMAGAZINE: What exactly does the eco Complaints Office do?

Alexandra Koch-Skiba, Head of the eco Complaints Office, explains the global cooperation of complaints offices, police and the Internet industry in taking child sexual abuse material offline.
ALEXANDRA KOCH-SKIBA: The eco Complaints Office deals with reports about illegal content, particularly content that is endangering (or might be endangering) to minors, and unsolicited emails people receive. Anyone can report potential illegal content to the eco Complaints Office and afterwards we deal with that by assessing the reported content from a legal point of view, and by tracing the hosting location.

There are two kinds of difficult reports: child sexual abuse material (CSAM), because it can be hard to cope personally, and hate speech, because of the quite difficult legal criteria.

DOT: What are the most difficult types of reports to deal with, and what makes them difficult?

KOCH-SKIBA: I would say that there are two kinds of difficult reports: The first one is about child sexual abuse material (CSAM), because it can be hard to cope personally with this kind of content and the images you see. The second one are reports about hate speech online, because of the quite difficult legal criteria that have to be met to be completely illegal, so the legal assessment is quite difficult. We are also dealing with different legal frameworks in the different countries with regards to hate speech, so in the end it is more difficult to take appropriate measures.

We offer psychological support, so if our staff want to talk to someone who is specialised to prevent traumatic problems, they can do that.

DOT: Processing complaints of illegal content is in some situations a very difficult task. How do you keep your staff from becoming too heavily burdened by this?

KOCH-SKIBA: We have a staff-welfare policy in place that is reviewed and updated every two years at least. If there are some important changes we are aware of, of course we update it sooner. We are reducing the time people have to see content, so there is a maximum time-period for every staff member to deal with reports per week; and we take care that people have the support they need before they develop problems. For instance, we offer psychological support, so if people want to talk to someone who is specialised to prevent traumatic problems, they can do that.

DOT: There has been a lot of talk about hate speech in the last couple of years. What measures are you involved in for dealing with hate speech?

KOCH-SKIBA: When we receive a report about hate speech, we process the report like any other report we receive – that means we make the legal assessment, we trace, we ask for appropriate measures – which can mean taking content down – and, of course, we notify police of illegal content. From a more political point of view and the lobbying work eco is doing, we are involved in several roundtables and discussions that are ongoing, to make clear that hate speech is not a usual complaint, that it is not the same as CSAM, for example, because of the different legal backgrounds we have. Of course, it makes a big difference if content is illegal in almost every country – you can have much faster success at the end of the day – which means the taking down of the content. But – with regard to hate speech – if content is legal in some countries, we somehow need to respect this as well. Providers are also able to take that content down when they cover this action in their terms of service, so even in that regard we can have success at the end of the day – but if there is no coverage by law or terms of service, we know it might be problematic for providers to take content down.

DOT: What kinds of law enforcement agencies does the Complaints Office cooperate directly with? Which other ones perhaps more indirectly?

KOCH-SKIBA: We have a very close collaboration with the German Federal Police Office (BKA). In regard to child sexual abuse material, we have a written MoU, and there are several meetings with them to exchange expertise, to discuss problems and to find good solutions for everybody. In regard to hate speech, we have a kind of informal cooperation with the BKA – we can also reach out to them to make them aware of specific problems. In regard to other content which violates German criminal law, we just reach out to the local police and notify them.

We know that there are differences in law internationally, but we want to give the provider the chance to see if there is a violation of their terms of service.

DOT: The Internet is a global infrastructure, and content could be hosted anywhere. How do you go about dealing with cross-border issues, either within or outside of the EU?

KOCH-SKIBA: When making our legal assessment, of course, we have German law as a benchmark because we are located...
in Germany, and our staff is educated in German law. So that is the starting point for us. If we see a violation of law then we reach out to the provider, in Germany, in Europe, but also outside of Europe. We know that there are differences in law, but we want to give the provider the chance to see if there is a violation of their terms of service, so they can take appropriate measures. In the end, there is no big difference in notifying the provider, but of course [there is] in regard to our expectations at the end of the day of what the provider is doing. When it comes to measures, we accept differences in law if we are aware of them. And when it comes to international cooperation, we also have partner hotlines around the world. We can reach out to them, ask for their specific expertise and knowledge, and ask them to go forward with reports – so they reach out to their cooperation partners.

Today, we have more than 50 partner organizations around the world – which means also in the U.S., Taiwan, in New Zealand, in South Africa... on almost every continent.

DOT: The Complaints Office is a member of the INHOPE network. Can you tell us a bit about the INHOPE network itself and how it functions?

KOCH-SKIBA: INHOPE was founded almost twenty years ago; it was actually founded in 1999, so a long time ago. Hotlines started to cooperate with each other, particularly in regard to child sexual abuse material, exchange expertise, but also to exchange reports. This means if we see content that is hosted in the UK, for instance, we reach out to our partner organization in the UK, asking them to take over the report and take the measures at a local national level. The cooperation with national partners is key in fighting illegal content – that’s our experience, and that is why we think that it is very important to have a network to cooperate with. There were seven or eight founding members at INHOPE, and it has expanded the membership significantly over the years. Today, we have more than 50 partner organizations around the world – which means also in the U.S., Taiwan, in New Zealand, in South Africa... so you can say that on almost every continent we have partner organizations, and we can reach out to them. The network itself needs a lot of trust because we can only report such content to trust-worthy partners – imagine we would send child sexual abuse material to someone who has a sexual interest in children: that would be the worst-case scenario I can imagine. So, it is important to have trust to each other, to have a kind of same level of knowledge when it comes to legal assessments and tracing – that’s very important. That’s why INHOPE itself organizes several meetings a year to exchange expertise, to know each other in face-to-face meetings, and it supports the hotlines through providing tracing courses or other training events, online and offline.

It is much faster to work with hotlines and the self-regulatory approach... and being fast when it comes to illegal content is important.

DOT: The eco Complaints Office is based on the concept of the self-regulation of the Internet. How important in your eyes is the self-regulation of the Internet?

KOCH-SKIBA: Self-regulation of the Internet is very important. It is not only the basis of the eco Complaints Office [but even more] it is the approach of our members. Many years ago, they talked about the best way to fight illegal content, and one of the results was the founding of the eco Complaints Office, and we still stick to the self-regulatory approach. So it’s us who inform the providers, instead of governmental authorities or something like that. Looking at the governmental authorities, you can say that it is much faster to work with hotlines and the self-regulatory approach than going the governmental ways. The way we cooperate with the providers is more informal – there are no procedural ways we have to follow, we can just reach out, notify them, explain why we think something is illegal and ask for measures to be taken. It is a very, very fast approach, and being fast when it comes to illegal content is one of the important things. So, it’s a very easy way to cope with illegal content. On the other hand, without self-regulation, when it comes to specific topics, new trends or something like that – the good cooperation often leads to a fast solution.

The domain name system is in good health. But it’s about to get even better. Mason Cole, Chair of the DNA Healthy Domains Initiative Committee, explains.

The Domain Name Association (DNA), the Internet domain industry’s trade association, undertook an effort in 2016 it named the Healthy Domains Initiative (HDI). It’s an ambitious, self-motivated effort to build on the DNS’ already secure and stable platform and meet select challenges head-on, before they develop.

While HDI is designed primarily to advance the safe and beneficial evolution of the domain name system, its secondary goal is to demonstrate to Internet stakeholders the capability of industry operators to effectively self-regulate. HDI is not under the aegis of ICANN or any other regulator — it’s an industry-led program that operates independently, guided by the organizations that have the operational experience to help keep the namespace healthy.

How HDI came about

DNA members, as stewards of the naming infrastructure, have long been attentive to ensuring their customers and Internet end-users have a safe experience with online identities. This became more the case with the proliferation of new top-level domains (TLDs), when so many new registries joined the community.

Interested DNA members persuaded the organization to form a committee to take on the project and outlined the following objectives:

- Establish a network of industry partners that communicate and collaborate with one another to support a healthy domain name ecosystem.
- Identify and/or develop industry-accepted healthy practices and specific programs that provide tangible ways of promoting standards for healthy domains.
- Demonstrate to the community the ability to proactively self-regulate and otherwise fulfill stewardship obligations

After a year-long process of consultation with registries, registrars, law enforcement, civil society, child protection authorities, pharmaceutical experts, content providers and others, the HDI committee identified the program’s first deliverable: a set of “healthy practices” that members may voluntarily adopt in order to address or prevent various issues that arise in namespace administration.

78% of respondents said that their companies already employed healthy practices.

The DNA first surveyed its membership on what, if any, healthy practices already were employed by members, and further, regarding the appeal of proposed new practices. An impressive 78% of respondents said that their companies already employed healthy practices outside the scope of their contracts with ICANN.

89% of respondents said they intend to expand this list to include additional practices. However, the conclusion of the survey, agreed to by most involved in HDI, is that there existed an opportunity to expand practice ideas, and contracted parties were receptive to doing so.
Healthy practices bring HDI to public notice

On February 8, 2017, HDI made its formal debut by publishing the first set of recommended healthy practices, a set of 37 total recommendations grouped into four areas that address:

- online security abuse;
- child abuse mitigation;
- complaint handling from illegal online pharmacies; and
- online copyright infringement.

The belief was that these four areas present a good avenue not only for establishing HDI, but to have an immediate impact on areas of known persistent issues.

In the days following the public launch of these practices, we received initial feedback about concerns regarding the proposed system for adjudicating copyright infringement (seven specific recommendations)—that feedback began to overshadow the other 30 practices advanced by HDI.

The DNA will take a keen interest in any provider’s considered design and use of a copyright dispute resolution system.

While addressing illegal behavior remains a priority of HDI, we accordingly elected to take additional time to consider the details of the recommendations. Thus, the DNA will take a keen interest in any provider’s considered design and use of a copyright dispute resolution system, and will monitor its implementation and efficacy before further refining its recommendations.

The DNA’s Healthy Practice Areas for Domain Registries and Registrars

HDI practices are focused on:

- Addressing online security abuse (e.g., malware, phishing, pharming) — this area encompasses 20 voluntary practices for registrars and registries to employ as means for combating domain name system (DNS) abuse. Recommendations include measures to mitigate abuse, receive and handle abuse reports, and otherwise minimize risks associated with potentially compromised domains.

- Enhancing child abuse mitigation systems — the DNA proposes that registries and registrars put in place a formalized system for handling of abusive child imagery, and establish “trusted notifier” relationships with child protection authorities.

- Streamlining complaint handling from illegal or “rogue” online pharmacies — these measures are designed to enhance registry and registrar capability to field, evaluate and handle complaints regarding online outlets suspected of being unlicensed pharmacies or otherwise distributing harmful or counterfeit medication.

Next steps

The HDI committee briefed DNA members on the final details of the plan during the NamesCon conference in Las Vegas in late January 2017. Members also heard from companies with a successful track record of implementing voluntary measures to combat abuse, as a point of reference for how to move forward.

As member companies voluntarily implement measures, the DNA plans to collect and make known examples of the efficacy of healthy practices, so the Internet community can understand the impact of these measures and contribute additional ideas. The HDI committee also looks forward to considering additional measures to contribute to the healthy evolution of the Internet namespace.

Read the article online here: https://www.dotmagazine.online/issues/who-rules-the-internet/who-rules-the-internet/HDI
INTERNET GOVERNANCE: BRINGING ORDER TO THE “DIGITAL WILD WEST” FROM THE BOTTOM UP

The strongest argument in favor of bottom-up, multi-stakeholder governance is that it actually works. Vittorio Bertola from Open-Xchange explores why self-regulation of the Internet is better than the alternatives.

When the Internet first became a mass affair, a little more than twenty years ago, all of a sudden the technical, netiquette-prone crowd of Internet pioneers found itself swamped by all sorts of newbies that seemed unable to behave. People from those times will remember that September 1993 never really ended; soon, having spam in the inbox became a normal fact of life, and the beautiful country of Nigeria suddenly filled up with people looking for strangers that would accept some free money.

As spam, fraud, flames, and cyberbullying became more common, people started to complain about the “digital Wild West” where no law seemed to exist.

Initially, the old Internet folks did not take it seriously. As early as 1996, John Perry Barlow’s Declaration of Independence made it clear that the Internet was considered to be out of the reach of the world’s governments. That, however, was just so wrong! In the following years, it became clear that governments had the opportunity to regulate, and even disrupt, the Internet. In many countries, servers were seized, dissidents were arrested, free software was legally attacked, users were intercepted, digital rights were taken away; though several good laws were also passed, including those protecting our privacy.

However, at the same time, the industry, the users, the developers, the leaders managed to explain to the world that the Internet was one of the best instruments for change, progress, and growth that mankind has ever invented. While some people and some governments really thought that the Internet should work like an updated telegraph or television network, with strict rules for everything and someone giving orders to everyone else, most were convinced that freedom of innovation and unfiltered communication are a boon to everyone (except, maybe, monopolists and dictators).

Starting from the “rough consensus and running code” principles of the technical working groups, the culture of “multistakeholderism” emerged; the idea that the Internet, as far as possible, should not be governed by hard law, but by soft law, by dialogue and cooperative action between public and private actors, including governments, businesses, civil society, and the technical and academic communities. And even if the early experiments at ICANN did not always go...
well, even though sometimes no hard law meant that private interests took control of some parts of the net, even though new governance issues arose every time the old ones were eventually sorted out, the Internet is still going strong after all this time.

The strongest argument in favor of bottom-up, multi-stakeholder governance is that it actually works.

The strongest argument in favor of bottom-up, multi-stakeholder governance is that it actually works; it exploits the networked intelligence of many parties to come up with solutions that address issues effectively. This also implies an important warning: if the Internet's self-governance does not work, sooner or later the governments will step in and will force hard rule on everyone; and usually—as this rule will not have been discussed with everyone and will be subject to the struggle for easy popular (populist) consensus that is typical of today's politics—this rule will be worse than it should be, and sometimes it's really bad.

This is why all sane and intelligent netizens, be they individuals, companies or other types of organizations, should be willing to put some effort into addressing open governance issues on the Internet—even the ones that do not directly and immediately affect the bottom line of their budgets. In the long term, a self-governed open Internet is going to be better for everyone, including those who make a living out of it.

...we do not just state our belief in an open Internet, but we try to put our energies where our mouth is.

This is also why, at Open-Xchange, we do not just state our belief in an open Internet, but we try to put our energies where our mouth is. As we make some fundamental free building blocks of the net, such as Dovecot and PowerDNS, and as we power the email, collaboration, and domain name resolution of many of the biggest ISPs around the world, we put some real effort into making our software open, secure and free (as in free speech) as much as any company could.

Moreover, we also sponsor governance-oriented community projects—and we would like to do more of them! The Trusted Email Services (TES) project is a good example of this approach. In the last year, we toured several countries organizing roundtables with the biggest hosters and ISPs, providing a technical brief on current email security threats and technologies, and encouraging participants to discuss and agree on common action.

Email security, in particular, is a field that can only advance by bottom-up cooperation. Whenever you write an email to someone else, that message has to be transmitted from your ISP to the recipient's one, thus involving at least two different companies, possibly more. If you want to implement better security methods, all companies have to support them. No ISP can do this alone, at least not if you still believe in the traditional principles of the Internet. If, instead, you believe that a single company in Silicon Valley should provide email and online identity services for all of the seven billion people in the world, then it is another story; but I would not want to live with an Internet like that.

If you tell someone that it is very likely that all his email messages are being transmitted in clear text, or under weak, easily breakable encryption, he will be surprised and scared. However, that is exactly how it is today; and that is also a nice selling point for those who would like to replace the open, cooperative email architecture with private messaging systems, capturing users in their walled gardens. This is the reason why we invest our money in organizing the TES meetings, even if they are not bringing us any revenue.

If you are interested in our project, please take a look at www.tesmail.org and feel free to contact us—we could even work together to organize a meeting. However, in any case, we would love it if other people would do the same in other fields, trying to advance security, user-friendliness, privacy, and innovation for everyone, and ensuring that those who want to turn the Internet into a walled garden, be they governments or companies, will never have any compelling grounds to argue that the Internet's governance traditions no longer work.

Stay Open. OX

Read the article online here: https://www.dotmagazine.online/issues/who-rules-the-internet/who-rules-the-internet/digital-wild-west
The Internet is a contested space with numerous stakeholders with hugely diverse interests. dotmagazine’s Béla Herting explores why the Internet needs governing, what approaches exist, and who are the key bodies looking to shape today’s global Internet ecosystem.

... from small beginnings

The flourishing “dot com” industry and the massive proliferation and diffusion of information and communication technologies (ICTs) in the early 1990s marked the beginning of the transition to today’s global Internet ecosystem – understood here as a decentralized international system of interconnected, yet independent networks which operate on different sets of open technology protocols. Over the years, the Internet has significantly gained momentum as a universal information and communication medium that profoundly changed our conventional understanding of interpersonal communication, and empowered its diverse beneficiaries on an unprecedented scale with far-reaching implications.

An unfolding process that has rapidly expanded into almost all economic, social, and political aspects of human life — predominately due to its “unique combination of physical and virtual properties” (Nye, 2014:5 https://www.cigionline.org/sites/default/files/gcig_paper_no1.pdf) that enable a fast growing number of Internet users to communicate across large geographical distances in an instant, with almost no marginal costs (Horvath, 2014:2 https://www.bundestag.de/blob/195878/af1d82ca9f8950e2258fafa31806c979/internet_governance-data.pdf). It was estimated by the International Telecommunication Union (http://www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2015.pdf) that the number of Internet users rocketed from 400 million in 2000 to 3.2 billion by the end of 2015.
What’s at stake

A meteoric rise that has not gone unnoticed – it has profoundly influenced a wide array of economic, political, and social relations between a diverse set of stakeholders, including, for example, multinational companies (MNCs), Internet service providers (ISPs), national governments, intergovernmental organizations (INGOs), and non-governmental institutions. Beyond any doubt, today’s global Internet environment has become a contested space in which “political and economic power is unfolding” (DeNardis, 2014:1-5 http://www.jstor.org/stable/j.ctt5vkz4n), seeking to reflect “different perspectives, approaches, and policy interests” (Kurbalija, 2014:6 https://www.diplomacy.edu/sites/default/files/An%20Introduction%20to%20IG_6th%20edition.pdf) in context of interdisciplinary and on-going debates about, for example, freedom of expression vs. illegal content (e.g. fake news or child sexual abuse material); data privacy and promotion of digital innovation vs. preservation of national security against cyber-crime and international terrorism; knowledge (or information) commons vs. intellectual property rights.

Key debates: freedom of expression vs. illegal content; data privacy and promotion of digital innovation vs. preservation of national security against cyber-crime and international terrorism; commons vs. intellectual property rights.

What can be observed is that the different stakeholders seek to further consolidate an overarching governance framework that is able to (a) provide a platform of coordination and exchange of information; (b) to harmonize the various sets of interests and requirements of today’s growing online community; and (c) to formulate appropriate responses to digital challenges that by far exceed the territorially-bound capabilities of national governments, and thus require new governance structures based on a common vision of the future evolution of the Internet.

How can the Internet be governed?

Reflecting “a web of relationships among the many institutions, organizations and communities that have roles affecting the operation and use of the Internet” (https://www.icann.org/resources/pages/glossary-2014-02-03-en), the governance of the Internet is a complex field that aims to address global power struggles on how the Internet and its physical and virtual properties are being governed and institutionalized. From the very beginning, the term Internet governance was subject of partly diverging interpretations for which, over the years, various stakeholders have struggled to come up with a universal working definition.

In 2005, among the first, the UN-sponsored conference World Summit on the Information Society (WSIS) in Tunis formulated the following working 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 […] an essential element for a people-centred, inclusive, development-oriented and non-discriminatory Information Society. (International Telecommunication Union, 2015:75 https://www.itu.int/net/wsis/outcome/booklet.pdf)

There is no universally accepted definition of what Internet governance really implies.

It was an attempt to articulate an inclusive and open approach to Internet governance that reinforces the dialogue between all stakeholders involved, and to emphasize its central importance for a progressive and interconnected communication environment that allows diverging interests and perceptions to be respected and to flourish. However, there is, to date, no universally accepted definition of what Internet governance really implies.

Bringing the stakeholders together in Internet governance – some key players

Internet Corporation for Assigned Names and Numbers (ICANN)

Founded in 1998 by the U.S. Department of Commerce National Telecommunications and Information Administration (NTIA), ICANN is an international, non-profit corporation that is responsible for Internet Protocol (IP) address space allocation, protocol identifier assignment, generic (gTLD) and country code (ccTLD) Top-Level Domain name system management, and root server system management functions. In other words, this California-based multi-stakeholder organization operates what can be regarded as a global phone book that enables billions of Internet users to receive information on their end-user devices (e.g. smartphones and computers) by, for instance, translating domain names (https://www.de-cix.net/) into IP addresses (46.31.121.34). (See the interview with Sven-Holger Wabnitz for further information on the functioning of the Domain Name System,
In the past, ICANN was often criticized by the international community of nation states for being an only semi-independent stakeholder-driven organization, due to the privileged position of the U.S. Department of Commerce to coordinate and manage the Internet Assigned Numbers Authority (IANA) functions. However, in October 2016, after years of standstill, the legal contract that granted the U.S. government significant oversight over ICANN finally expired. This decision by the former U.S. administration was very well received by all stakeholders involved – a “significant step towards the globalisation of Internet’s core infrastructure” (http://www.epw.in/journal/2016/42/web-exclusives/internet-governance.html), and the “most advanced version of a multistakeholder mechanism for a free, open and unfragmented Internet” (http://www.circleid.com/posts/20160106_internet_outlook_2017_nationalistic_hierarchies_multistakeholder/). (For a detailed account of the IANA Stewardship Transition, see A Quiet Global Revolution, this volume, pg. 22) However, it must be seen that ICANN remains located within the boundaries of U.S. jurisdiction, meaning it is not immune to conflicting national interests and U.S. law.

eco’s Thomas Rickert (https://youtu.be/zO-iNihmXF0) and Lars Steffen (https://international.eco.de/2016/news/getting-next-billion-online-universal-acceptance.html) are regular participants at ICANN meetings on behalf of eco.

Internet Governance Forum (IGF)

Another important multi-stakeholder format is the Internet Governance Forum (IGF), a UN-related platform for dialogue on “public policy issues related to key elements of Internet governance issues, such as the Internet’s sustainability, robustness, security, stability and development” (http://www.intgovforum.org/multilingual/content/about-igf-faqs). It was established as a result of the UN-sponsored conference World Summit on the Information Society (WSIS) in 2005 – a non-decision-making forum that facilitates multi-stakeholder discussions about different public policy issues regarding core features of Internet governance (https://digitalwatch.giplatform.org/processes/internet-governance-forum). In line with its mandate, the IGF seeks to shape the evolution of the Internet by organizing regional, national and inter-governmental forums to encourage multi-stakeholder policy dialogues on an annual basis.

What is needed in today’s information age is a discussion platform that can be a meaningful tool to raise attention and support for Internet-related issues, and thereby structuring cross-national debates. According to Wolfgang Kleinwächter (http://www.circleid.com/posts/20160106_internet_outlook_2017_nationalistic_hierarchies_multistakeholder/), the IGF has finally reached a level of maturity which can further develop “Internet governance policy making [and] to kick start a discussion or to organize pressure towards decision-making bodies to find solutions for emerging issues” as could be seen during the IGF event in Guadalajara in December 2016. What is needed in today’s information age is a discussion platform that can be a meaningful tool to raise attention and support for Internet-related issues, and thereby structuring cross-national debates.

eco’s Chairman of the Board, Professor Michael Rotert (see Access, Human Rights and Getting the Next Billion Online, this volume, pg. 26), represents eco regularly at IGF meetings.

Internet Society (ISOC)

The Internet Society (ISOC) is a US-based non-profit organization that was founded 1992 with the mission to promote leadership for “Internet policy, technology standards, and future development [and] to ensure the Internet continues to grow and evolve as a platform for innovation, economic development, and social progress for people around the world” (http://www.internetsociety.org/who-we-are/mission). Governed by a diverse Board of Trustees, this membership-driven organization has currently more than 80,000 members and supporters, ranging “from non-profit agencies, local and global NGOs, academia, technologists, local councils, federal policy and decision makers, business and more” (http://www.internetsociety.org/who-we-are/our-members), as well as more than 140 organization members. (For further information on the Internet Society, listen to the interview with Olaf Kolkman, Chief Internet Technology Officer at ISOC, in A Day in the Life of a Man with a Key to the Internet, this volume, pg. 28)
International Telecommunication Union (ITU)

Founded in 1868, and thus considered as one of the oldest inter-governmental organizations, the International Telecommunication Union (ITU) is a specialized agency of the United Nations with the “mission to enable the growth and sustained development of telecommunications and information networks, and to facilitate universal access so that people everywhere can participate in, and benefit from, the emerging information society and global economy” (https://www.un.org/agency-itu.php). In short, the ITU has three main sectors that define its core focus:

1. Radio Communication (ITU-R)
   a. Managing the international radio-frequency spectrum;
2. Standardization (ITU-T)
   a. Maintaining standards for telecommunication services;
3. Development (ITU-D)
   a. Ensuring access to ICT for the developing world.

In contrast to ICANN or the Internet Society (ISOC), which pursue a multi-stakeholder approach based on private sector organization, the ITU working groups “represent a telecommunications governance regime that is international and centered on nation-states” (http://www.internetgovernance.org/2009/11/20/the-igf-and-the-internet-society-itu-rivalry/), which means that non-state stakeholders are still largely excluded from the public policy mechanism at ITU. These divergent approaches to Internet-related issues are supported by different nation states. For example, developed countries in the West, such as the U.S. and EU member states, tend to predominately advocate ICANN and ISOC, whereas the strongest support ITU receives is from countries that value national sovereignty in cyberspace, including Russia, Brazil, China and the Arab states (http://www.internetgovernance.org/2009/11/20/the-igf-and-the-internet-society-itu-rivalry/).

Beyond any doubt, most Internet-related issues require a more holistic approach that acknowledges its universal interlinkages and cross-national nature.

To address current and future challenges that emerge through the global environment of the Internet, the international community of nation states and other stakeholders involved need to further develop meaningful discussion and negotiation forums, where different interests, perspectives, and policy focuses can be expressed and harmonized. Beyond any doubt, most Internet-related issues require a more holistic approach that acknowledges its universal interlinkages and cross-national nature. Traditional power politics based on national sovereignty, territoriality, and the principle of non-interference will certainly remain ineffective to solve the Internet governance issues of tomorrow.

Béla Herting

Read the article online here: https://www.dotmagazine.online/issues/who-rules-the-internet/why-how-who-of-IG
WHO RULES THE INTERNET?

A QUIET GLOBAL REVOLUTION

Thomas Rickert of Rickert.net tells the story of the success of a revolutionary and promising model of global governance – as established through the ICANN IANA Stewardship Transition – and why you should know and care about the balance of power in Internet governance

March 14, 2014 was likely just another day for you, unless maybe it was your birthday.

However, for a lot of folks around the globe, this day was memorable or it became important to them subsequently – including myself. With this article, I would like to share with you how that day substantially impacted the world of Internet Governance and beyond. And what is so exciting about this is that the model of governance that evolved out of the process that began on March 14, 2014 has the power to change the way we manage global issues in future. A model which recognizes that it’s not only governments, and it’s not only multinational corporations that have a stake in global issues. It’s also the civil society – you and me of our world – who have a stake in the global future, and who should also have a say in how it unfolds. And so, if you take the time to read this, you might agree that March 14, 2014 changed a lot. Silently, almost unnoticed.

But let’s start at the beginning of the adventure: On March 14, 2014, the U.S. Commerce Department’s National Telecommunications and Information Administration (NTIA) announced its intent to relinquish its historical oversight role over the IANA functions to the global multi-stakeholder community.

The Challenge

The NTIA asked ICANN, the Internet Corporation for Assigned Names and Numbers, to convene a multi-stakeholder process to develop a plan for this transition. The plan the NTIA required had to have broad community support and meet the following requirements:

• Support and enhance the multi-stakeholder model.
• Maintain the security, stability, and resiliency of the Internet DNS.
• Meet the needs and expectations of the global customers and partners of the IANA services.
• Maintain the openness of the Internet.

The NTIA also stated that it would not accept a proposal in which the US Government’s (USG) role would be replaced by a government-led or intergovernmental organization.

The community started discussing how this job could be done and it quickly became clear that ICANN’s accountability should be enhanced so that the organization, and with that the important functions it performs, are protected from undue influence and risks to preserve the resiliency and stability of the DNS.

For those who are not familiar with ICANN or IANA, the IANA functions have to do with IP addresses, Protocol Parameters and Domain Names; the management of the Root Zone Database to be more specific. (https://www.icann.org/en/system/files/files/functions-basics-07apr14-en.pdf)

So what was the USG’s role and why did the USG have this role in the first place?

Before ICANN’s inception, way back when the Internet did not yet exist, but the ARPANET had started – a network funded by the U.S. Department of Defense – the IANA functions were performed by Dr. Jon Postel.

ICANN was formed as an organization based on a global bottom-up multi-stakeholder approach. This governance model was brand new at the time, and no one knew whether it would work. As a result, the USG retained authority over the IANA functions, but entered into written agreements and
contracts with ICANN on the mutual roles.

However, the oversight role was only planned to be temporary, so what happened in March 2014 was carrying through on a promise made by the USG more than a decade earlier.

**Why did the USG want to hand it over?**

The Bush administration did not make any efforts to relinquish the USG oversight role. Obama did and we do not know for sure what exactly triggered the process. Yes, the USG oversight role was only meant to be in place until such time that ICANN’s multi-stakeholder model had proven a workable approach, but that was surely not the only reason for Obama’s actions. The statement was issued at a time when Snowden had made his revelations and many countries were upset with the US control and surveillance of the Internet. With several governments going public with their intent to start their own Internet (I’m paraphrasing here) as a reaction, the USG announcement did help the USG to bring many countries back to the table and maintain a non-fragmented Internet.

**How important was this role?**

It is true that the USG did not play a huge role. In practical terms, it was more or less limited to signing off on requests prepared by the IANA team at ICANN on delegation requests for Top Level Domain Names. In other words: All the new Top Level Domain Names that were launched over the past few years need to go through this process and be entered into the Root Zone Database to be functional at the global level via the DNS. That was never a big deal and even TLDs such as the “virtual red light district” TLD “.xxx” were approved by the NTIA despite fierce debate in the US.

What was far more important was the threat that the USG held over ICANN – to go elsewhere to have the IANA functions performed if ICANN chose not to follow the USG’s directions or wishes. Indeed, the USG required ICANN to constantly work on its accountability and transparency, for example.

---

Today, we would likely call such a statement an “alternative fact”.

All in all, the IANA Stewardship Transition from the USG to the global multi-stakeholder community was given more weight than it should have from an operational perspective. But, the symbolic importance was and is huge, as for many it was tantamount to answering the question “Who controls the Internet?”. Some even went as far as claiming that whoever runs the IANA functions runs the Internet, and can regulate content. Today, we would likely call such a statement an “alternative fact”.

**A Herculean Task**

The community went to work. In fact, different actions were kicked off to work in parallel. Each of the three IANA functions had a team working on a transition proposal for
their respective areas. In addition a co-ordination team (called ICG) was set up to coordinate the proposals on Numbers Resources (delivered by the CRISP Team), Domain Names (delivered by the CWG-Stewardship) and Protocol Parameters (delivered by IANAPLAN). As a separate track, the CCWG Accountability worked on enhancements to ICANN’s accountability.

The community knew that the job needed to be finished before the end of the Obama administration, due to the uncertainty of whether a transition would be supported by Obama’s successor.

The community knew that the job needed to be finished before the end of the Obama administration, due to the uncertainty of whether a transition would be supported by Obama’s successor.

ICANN’s new gTLD program, which led to the introduction of more than 1,000 new generic Top Level Domain Names and which sparked off considerable debate about TLDs that were geographical names, generic terms such as corporate identifiers or relevant to regulated professions, has caused an increased interest by many public and private stakeholders in ICANN. Combine this with the huge symbolic value the IANA functions were given and it becomes obvious that a wide range of views was formed about how ICANN should be governed and who should have what power in controlling such a critical resource.

With the limited time given to come up with a proposal, many doubted that it would be possible for the global community to come up not only with a proposal, but with a proposal that was broadly supported.

A lot was at stake: Not only could the window of opportunity be missed to get the transition done, but, maybe even more importantly, the multi-stakeholder model would have proven to be inefficient and unable to deliver solutions to global challenges.

The biggest teams had more than 150 (CWG-Stewardship) and 200 (CCWG-Accountability) individuals working in them with backgrounds as diverse as can be. There were times where it looked like there were irreconcilable differences in opinion.

More than 1,100 meetings, more than 33,100 mailing list exchanges, more than 600 calls and meetings, and millions of dollars later, the task had been accomplished. The best possible legal advice was obtained to ensure all requirements and features that the community had established could be legally implemented.

It took the community roughly two years to work on and refine the proposals. There were multiple public comment periods in which input from everyone interested in the topic worldwide was solicited, analyzed, and considered for improvements of the proposal. Let’s not forget the existing ICANN structure and its Board, who also had firm views on how the organization should and should not be changed. Robust and, at times, high-handed discussions helped ensure that no stone was left unturned to explore what the best possible and most feasible solution to the issue should be.

Ultimately, ICANN submitted its report to the USG. It was assessed by the NTIA and even examined by a group of corporate governance experts including Columbia Law Professor John Coffee, Brooklyn Law Professor Dana Brakman Reiser, and The Berkman Center for Internet & Society at Harvard University to review the ICANN accountability provisions, who concluded that the accountability recommendations are consistent with sound principles of good governance. Thus, the NTIA announced on June 9, 2016 that the criteria established in March 2014 were met.

Well done, you might think. But not everyone did.

Oh no, not another hurdle!

Those who opposed the transition used propaganda to try to prevent it from happening. They tried to establish a law that would have made it harder. They tried to render it impossible by means of budget allocation for the NTIA (or lack thereof), and they even took it to court. “Barring any significant impediment”, the NTIA’s plan was to let the existing contract
with ICANN on the IANA functions expire by the end of September, 2016. Only on the last day of September was the application for a temporary restraining order preventing the transition from taking place rejected by a judge in Texas. 

Sigh of relief

**What’s been called the Empowered Community now has ultimate control over ICANN and the IANA functions.**

ICANN became independent of government oversight as of October 2016. It was a close race, but all the controversy made it even stronger. What’s been called the Empowered Community now has ultimate control over ICANN and the IANA functions. The Board or Board members can be removed if need be, ICANN and IANA budgets can be rejected, as can strategic and operating plans, bylaw changes can be controlled, a binding and improved Independent Review Process has been established, amongst other things. The full several-hundred-page report including summaries and graphics can be found here: https://www.icann.org/resources/pages/board-ntia-transmissions-2016-06-13-en.

Outlook

The transition was successfully completed, but more work needs to be done. The accountability work still needs to be finished, as only those accountability enhancements that were directly related to the transition had been worked on in the first phase. Now, work on important topics such as diversity, transparency, and certain aspects of jurisdiction are still under way. Also, the different parts of the community, such as the Governmental Advisory Committee, the Generic Names Supporting Organization, the At Large Advisory Committee, the Country Code Names Supporting Organization and the Address Supporting Organization are in the process of synchronizing their own operating methods with those required in the new ICANN.

---

**We need multi-stakeholder responses to a multitude of global issues.**

The most important aspect, though, is that a global community of officials and volunteers with very diverse backgrounds came together and found a consensus solution to a global issue. Their dedication and tireless efforts were nothing short of remarkable and therefore the IANA Stewardship Transition deserves to be the role model for functional multi-stakeholder work. We need multi-stakeholder responses to a multitude of global issues. ICANN is not the place to solve those issues, but it has created a blueprint of how problems can be tackled and resolved in a relatively short period of time.

Have we made everyone happy? No, far from it. Nobody got everything they wanted, but we have made everyone equally unhappy. That's what makes a good compromise.

Thomas Rickert, Attorney-at-law and owner of Rickert Rechtsanwaltsgeellschaft mbH, Bonn, Germany (rickert.net) chairs eco’s Names & Numbers Forum (https://numbers.eco.de/international.html). He is one of three co-chairs of the CCWG-Accountability (https://www.icann.org/stewardship-accountability).

Read the article online here: https://www.dotmagazine.online/issues/who-rules-the-internet/why-how-who-of-IG/a-quiet-global-revolution
ACCESS, HUMAN RIGHTS, AND GETTING THE NEXT BILLION ONLINE — THE IGF AS A GLOBAL MULTI-STAKEHOLDER PLATFORM

Prof. Michael Rotert, Chairman of the Board, eco – Association of the Internet Industry

Prof. Michael Rotert, eco Chairman of the Board, explains the workings of the Internet Governance Forum as a Global Multi-Stakeholder Platform

The UN’s Internet Governance Forum (IGF), a multi-stakeholder platform that facilitates the discussion of public policy issues pertaining to the Internet, usually focuses on access to the Internet as a human rights issue, rather than Internet usage. It is an issue not just for users and civil society, but also for those representing the Internet economy and the technical infrastructure behind the Internet. The IGF is a powerful platform for civil society, as it is a rare opportunity to share a forum for discussion and possible influence with technicians and government representatives.

Free access to information and affordable access to the Internet are important human rights issues that the IGF addresses.

One frequent topic of discussion is trans-border Internet, in particular “locked countries”, so when information in or information flowing through a country is modified, blocked, or otherwise obstructed in some way, sometimes with the support of a third party or another country. The discussions do not necessarily lead to policy changes, nor can a country be forced by the international community to stop blocking the Internet or electronic communication, but it does create a space to build public pressure on such countries, which in turn can give impetus and support to pressure groups and civil society in these countries.

Other bodies, such as the Council of Europe (https://www.coe.int/en/), do very valuable work on human rights for Internet users (http://www.coe.int/en/web/internet-users-rights/guide) and they are really shaping the dialogue in the international arena. The IGF builds on such work and often brings in other perspectives and other voices. The Council of Europe’s work is often focused on legal issues, whereas the IGF is quite strong in addressing the technical aspects and the views of the civil society.

IGF 2016 Meeting in Guadalajara, Mexico - Session of the German Community

Free access to information and affordable access to the Internet are important human rights issues that the IGF addresses. Also discussed are cultural questions related to the Internet on a country level. These are usually discussed in special sessions organized by regions. There can be very heated debates on whether and how, for example, religion and churches should be present online.
The IGF has a focus on developing a set of policy options aimed at the creation of enabling environments to help get the next billion Internet users online.

Affordable Internet access is a huge issue for developing countries. While access may be technically available due to often very good mobile coverage, mobile Internet access is usually substantially more expensive. The IGF started an intersessional project "Policy Options for Connecting the Next Billion" (http://intgovforum.org/cms/policy-options-for-connection-the-next-billion#framework) in 2015, focused on developing a set of policy options aimed at the creation of enabling environments to help get the next billion Internet users online.

The IGF has changed the format of its forums to open up more to stakeholders who cannot attend the meetings. The discussions during the forum are live-streamed so interested individuals can follow the sessions in real-time online. In future, each session will have a rapporteur who will be responsible for summarizing the session proceedings and making these available online. Disseminating the discussions, debates and findings of the IGF is a priority.

Michael Rotert will be representing eco at the next IGF meeting in Geneva, Switzerland on 12-14 December 2017.

Read this article and listen to a related short interview with Prof. Michael Rotert online at: https://www.dotmagazine.online/issues/who-rules-the-internet/why-how-who-of-IG/igf-and-human-rights
A DAY IN THE LIFE OF A MAN WITH A KEY TO THE INTERNET

For most of us, the Internet is that magical connectivity that somehow emanates from plugs in the wall, yet it is a vast global network of interoperable networks, geographically distributed, and robust enough to withstand nuclear attack. dotmagazine’s Judith Ellis talks to Olaf Kolkman of the Internet Society about the Domain Name System and his key to the Internet.

DOTMAGAZINE: As one of the seven main keyholders protecting the DNS root zone, you literally and metaphorically have one of the keys to the Internet in your hands. What would be the repercussions of these keys falling into the wrong hands?

OLAF KOLKMAN: I’m going to push back a bit on the assertions made in the question. First, it’s not the keys to the Internet. What I’m involved in is the protection of the so-called DNS. DNS is the highly distributed system that translates names that we use on the Internet, for instance the domain names that you use in email addresses, or the domain names that you use in browsers, to the IP addresses and other resources that computers need to do their job. Metaphorically, people refer to it as a telephone book.

The structure of that system is such that it is highly hierarchical. There is a so-called root zone, which points to the location of the next level down, which are the top-level zones. The root zone knows where to point somebody – which is a machine that usually lives in your local network – and it refers that machine to the next level down, say, .nl or .com. Then .com will refer further down to the machines that know where, say, the cocacola.com company is, or where isoc.org is. So we’re talking about the root of that system, and the signatures that are provided there are signatures that provide authenticity and integrity of the information. They basically sign off that the information you pass by hasn’t been modified and is published by the right entity.

That system is in place because otherwise, the information that traverses the Internet – all the questions and answers – might be replaced by somebody in the middle who tries to muck with that resolution. If that happens – if somebody mucks with that resolution process – you might end up with the wrong party to talk to. For instance, you think you are talking to your bank, but instead you might be talking to another service. You type in your bank address in your web browser, there’s a look-up, the information is being replaced, and you talk to the wrong entity. There are other protection mechanisms that will flag that, but you want to have that protection throughout the Internet architecture, at every layer of this structure.

This is what we’re trying to protect. The keys that are used to generate these signatures are stored in machines called hardware signing modules. They’re baked into a chip, so to speak. And there’s a little bit of a layering here: there’s a master key, which lives in a machine that lives in a vault, and that master key is removed from that vault once every six months to generate signatures of the production keys that are maintained to be more accessible by somebody who operates the root zone.

So, these keys are sort of master keys, they live in a device that sits in a vault. That vault has very high security perimeters. In fact, there are seven layers of security, and you cannot get into that vault without being seen, without having to sign in, without collaborating with other people. My role in that whole process (and I’m not one of seven, I’m one of fourteen, because there are seven on the east coast and seven on the west coast) is to carry around a small key which can open a de facto safety deposit box. And in this safety deposit box in a tamper-evident bag, is a smart card.

Olaf Kolkman, Chief Internet Technology Officer, Internet Society
There are seven smart cards in that vault, in that facility, locked behind seven doors. In fact, my role is – with my little physical key, because I have a physical key – to open that little vault, take out the smart card, look at whether that smart card or the vault has been tampered with, very carefully study that tamper-evident bag, very carefully look that it’s not ruptured, and make sure that there is a continuity in the procedure so that if somebody ever had their hands in the vault and drilled out the lock or opened it, I can see that. I am an observer of a process that is meant to audit the integrity of that root key, and audit that nobody has gotten access to that key in the last six months.

DOT: Have you ever had any evidence of tampering for any of the keys?

KOLKMAN: No. That is an unequivocal no. There has not been any evidence of that. And obviously, if that ever happened, any of the keyholders would be extremely vocal about it.

The reason why we have those keyholders is that three out of seven independent people need to get together in that vault, get through those seven layers of security – which they can only do with other people being present, like staff from ICANN – to first open all the locks that get us into that vault so that we can open our little boxes and take out the cards.

Those cards are then presented in a ceremony which is precise and very well structured. And by the way, publicly broadcast: everybody can watch the broadcast of these ceremonies. The goal is to be extremely transparent in the management of the key, so that at the first suspicion that something went wrong, we can expose it.

If that ever happened, that would be a blow to the trust in the Internet. What we’re trying to do collectively as a community is to be as transparent as we can in showing that there is continuity and that the key is secure. While protecting the bits that generate the signature. That is something that is very important.

DOT: How is the Domain Name System protected?

KOLKMAN: It’s a fairly complex system that as I have described, has these layers of delegation. If you look at a domain name, www.internetsociety.org, the root is responsible for maintaining who has the information on the org level. At the org level there’s an organization that is responsible for maintaining the information at the layer below it. An organization like the Internet Society maintains the information about the internetsociety.org domain. As you see, there are already a few entities that have responsibility. If you, as a customer, use your iPhone or your computer, there is a machine in the local network that will go and hunt for the answers that you are asking. Those machines are called resolvers.
The way that we have protected the Internet Domain Name System, metaphorically, is that the messages that get passed by all these machines—or the information that is transferred over the Internet can be considered as if they are postcards. And a postcard can easily be lost if we don’t protect against that. The other thing is that everybody can read what is on the postcard while it’s in transfer. For example, the postman can look at the postcard and see the address and the little memo that you’ve put on the postcard. It’s not something that we protect against – at least, not with DNSSEC.

In essence, what we are doing is putting those postcards in transparent envelopes, closing the envelope and putting a seal on it.

In essence, what we are doing is putting those postcards in transparent envelopes, closing the envelope and putting a seal on it. And by looking at the stamp of the seal, you can tell who sent that envelope. You know who the holder of the seal is, and you can look at the seal and say, ok that was the .org domain that sent me that information. And I know, because this envelope is completely intact, that the message has not been tampered with. Nobody tried to write something else on the postcard that would cause confusion on the resolver or customer end.

That is the concept. In this system, the root zone puts a seal on the message to say “the org zone has information about internetsociety.org, go there.” And on the postcard, inside the envelope, it puts what the seal that verifies .org looks like. So, the resolver then knows –look at the postcard, the next seal that I’m expecting looks like this, I can verify the next signature that I’m expecting against this image. At the top-level domains that really works well. There are a few hundred domains in the world that are signed and that deploy DNSSEC. On the lower level, however, there is not that much uptake. In the Netherlands, the uptake is very high – a few million domains are signed. In other parts of the world, the success rate of creating and maintaining those signatures, is not very high.

...almost everything we do on the Internet starts with a DNS query. Being able to validate that nobody tampered with that is incredibly important.

So that answers the question of how well the DNS is secured: not very well, because there are not that many signatures around. And this is a point of concern. In the Internet, we sometimes find it hard for people to invest in the security of others. And this is an investment. Creating signatures is really an investment for any of the entities that need to do it. It doesn’t introduce immediate visible effects –having a signature doesn’t change the quality of your service and it’s not even visible to the end-user. I as an end-user, you as an end-user, and all of our readers and listeners – they don’t see anything about the DNS. And that’s good – they shouldn’t need to know about the inner workings of the system. But it also means that there’s no financial benefit in applying those seals, because they are not visible to the end-user. I think that is an issue because this whole infrastructure – almost everything we do on the Internet – starts with a DNS query. Being able to validate that nobody tampered with that is incredibly important.

And once you have that infrastructure in place, you can actually innovate on top of that. And what you see nowadays is that there are innovations: for example, when I want to set up an encrypted connection with you, and I don’t have any a prior knowledge about you, how do I do that? Where do I get that information? If we have a secured DNS, it could be a source for that information. In some cases, it could be a secondary source of information so that you compare the results that you get from one source with another – which enhances technical trust. I think we need to collectively pay attention to these technologies and take our collective responsibility in deploying them.

DOT: How often do you attend the Key Signing Ceremony, and what is your most memorable incident relating to it?

KOLKMAN: The Key Signing Ceremony takes place every year: once on the east coast, and once on the west coast. I’m a ceremony participant keyholder for the east coast facilities. The Key Signing facilities are in Culpepper, Virginia – a big data center where there are also a lot of federal and payment industry facilities. It was put there to be outside of the nuclear blast zone for Washington DC.

I attend as much as possible, because I feel my responsibility there is to audit the processes and to make sure that they are followed.

We need three out of seven participants in the key ceremony in order to do a successful transaction. Personally, I believe that we should have five out of seven to validate that no three keys have been used in combination in the interim. I try to attend as many times as my schedule permits. There
will be a key ceremony in April (27th and 28th) 2017, and there will be six keyholders there. I attend as much as possible, because I feel my responsibility there is to audit the processes and to make sure that they are followed.

Obviously, the first ceremony was very memorable – as a sort of a piece of history. That was a very important piece – the introduction of the key. The last was also memorable because we introduced a new key into the system. One thing you have to know about cryptography and cryptographic keys is that they have a lifetime. It is wise to replace a key that is used for creating signatures every now and then, because they might be brute-forced. At the last ceremony, we introduced a key that is going to be used to sign a new key set in April 2017, and that new key set will be introduced into the root zone on July 11 2017. That is the first time that we're going to roll the keys of the root zone, and that's a somewhat scary moment.

It's very important for the people who maintain these resolver boxes that do validation to be aware of this change and make sure that their resolver tracks that change.

The reason being: I mentioned that at the customer side, we have these resolvers that do the validation of those seals. Now, they all have an idea of what the seal of the root – the highest point of the hierarchy – should look like. There is a procedure and a published technical specification that allows for replacement of the seal in the resolver through a special process. What we do not know is whether all of the resolvers out there actually implement that technical measure to track that change of the seal. What is a little bit scary in this whole thing is that when that seal is removed, maybe some of the old resolvers are still out there at the customer premises trying to validate against an old seal that they've never replaced. So it's very important for the people who maintain these resolver boxes that do validation to be aware of this change and make sure that their resolver tracks that change. Otherwise, their customers will not be able to do look-ups against the Internet and will therefore de facto drop from the net.

It's also important for anybody who does DNSSEC validation to make sure that they're implementing the automatic roll-over technology, which we refer to as RFC 5011, and if not, that they do a manual reconfiguration. Obviously, this is an ask for specialists – this is not something that non-specialist users would need to do at home. It's really the people at ISPs and mobile operators and whoever runs such validating resolvers. The people who run a validating resolver at home, I consider specialists – they know the plumbing [laughs]. And actually, that is possible – you can run this type of infrastructure yourself. If you don't trust others to do the work for you, the beauty of the Internet is you can always do it yourself.

Those type of things might cause delays... but in the meantime, we're all locked in this room.

DOT: Still talking about the Key Signing Ceremony, which security measures do you find most inconvenient?

KOLKMAN: The ceremony itself is a bit tedious as it's long and it's very precise. We're following a script, and every exception to that script is noted and actually assessed – whether there's a security implication, or whether we're doing the right thing – and there is an auditor that follows the script and makes sure that those exceptions are noted. We have had cases where, for instance, the person who had to open the vault got a bit nervous. There are dial locks, and you have to be very precise – if you overshoot, you have to start again and, as far as I understand, if you do that a few times, you have a time-out of five minutes, and if you do it wrong again then the time-out is even longer. Sometimes those type of things might cause delays and cause an exception to the script – which is, again, very transparently assessed, written down for everybody to see, it's on camera – but in the meantime, we're all locked in this room. What we do, if these ceremonies are very long, then we make sure that people can go out of the room, and we actually bring in an armed guard that guards the key material – again, somebody who is completely independent of the process.

DOT: So, how did someone who studied astronomy end up becoming a central figure in Internet administration? How and why did you become a keyholder?

KOLKMAN: A long story short: Starting with astronomy, it's not uncommon for physicists and astronomers to work with modern computer technology – that's always been the case. Astronomy has traditionally been a topic of Big Data – regardless of the times, it was always the biggest data...
around. Physics too. Whenever there was an opportunity to do Big Data and transfer data around, astronomers and physicists are the first to knock on the doors. You still see that academic networks are at the forefront of technology in that sense. And as an astronomer, as a student, we all had to put our weight behind maintaining some of the infrastructures, so I got interested in basically maintaining pieces of infrastructure. Got interested in the world-wide web – the lab introduced an http server, and volunteered to install that and maintain the information, and so on. So I slowly gained expertise with Internet technology, found it pretty interesting, applied for an Internet job while I was working on my PhD, walked away from my PhD, and got into an Internet environment.

I was very lucky to work with the right people to have access to knowledge, expertise, and leadership to learn on the job.

My second job in that environment was the RIPE NCC, which is one of the core Internet institutions, and I was very lucky to work with the right people to have access to knowledge, expertise, and leadership to learn on the job. One of the things that Daniel Karrenberg of the RIPE NCC felt very strongly about was leading by example. In early 2000, when DNSSEC was thought to be done, he said Olaf, I have a project for you – please go ahead and try to learn everything you can about DNSSEC and then teach that to our membership. I did that in cooperation with a group called NLnet Labs, and what we in essence discovered was that the DNSSEC protocol at that time was just not finished. So we had to go back to the drawing board, and I got involved more intensively in the work of the IETF – the Internet Engineering Task Force. I became Chair of the working group that worked on the DNSSEC extensions, also continued to work on the technical side trying to sort out solutions, worked with the people at NLnet Labs to build a name server – all those things happened sort of at the same time.

Then I made a move and became Director of NLnet Labs, was also involved in the IETF leadership, member of the IAB (Internet Architecture Board), so sort of a visible person in the community. And since NLnet Labs did one of the first – actually the first – by design DNSSEC name server, we had the technical background and credibility in the community, and when the NTIA and ICANN at the time were looking for volunteers with a credible background and support of the community, that was a logical step.

DOT: Tell us something about your work for the Internet Society – what does the Internet Society do, and what is your role?

KOLKMAN: The Internet Society is a global organization, and what we are about, essentially, is the open Internet and protecting the opportunities that the open Internet brings to society. We are a membership organization – there are 234 countries and territories that have ISOC members, membership is well into 90,000. Members are often organized in chapters, which are sort of independent groups that subscribe to our mission – the open Internet – and try to work within their local communities to push and implement that agenda. There are 125 of them, in 105 countries. And then we have organizational members that support our cause – of which there are over 130.

We have a staff that focuses on development and access, making sure that people have access to the Internet – an Internet that brings those opportunities – because we believe it is a vehicle for human development.
We have a staff that focuses on development and access, making sure that people have access to the Internet – an Internet that brings those opportunities – because we believe it is a vehicle for human development. We believe it’s a vehicle in achieving policy goals like the sustainable development goals set by the UN. We support a technical agenda – we’re the organizational home of the IETF, the standards organization for the Internet, and we provide funding for that and some organizational support. Obviously, the IETF itself sets and drives its own agenda – we’re not a part of that. It sets its own culture and standards and rules and internal procedures, but we do support them with finding sponsors, with financial continuity and so on.

We have our own technical agenda: we’re trying to move technology in a way – or trying to convene technology communities in a way – that they enhance, for instance, the trust in the Internet. Our main areas of focus with respect to the Internet are trust and access. So, getting people connected, and making sure that they can keep trusting the Internet. For example, DNSSEC is one of the things that we continue to inform people about, we keep measurements on what the amount of deployment is, and try to give practical information to the people that have to deploy this technology through our Deploy 360 channel. We also promote IPv6 – the new (not so new any more) addressing scheme that allows more than four billion people to connect with IP addresses. As you may know, the IPv4 addresses – which is the Internet’s addressing scheme on which the Internet has run for forty years – have run out, and the transition to a new set of addresses – IPv6 – is an important piece of our work. We try to inform people who have to do that work on how to do that best, and organize communities around that.

So we can have safe conversations, secure bank transactions, we can do our business in a trustworthy way: those are things that we care about and we want to create a policy environment and a technical environment that allows that environment to prosper.

The ability to innovate, the ability for new entrants, the ability for new ideas – those are things that we care about deeply at the Internet Society, and we are trying to do that through a development agenda, sponsoring local initiatives, a technical agenda, bringing communities together, organizing sessions around difficult questions, and by having a policy environment in which all this can work. We’re also informing and educating policy makers about the deep workings of the Internet. And that’s an incredibly fun job. My role, by the way is Chief Internet Technology Officer, so I’m looking at what we do in the technology agenda for that, and partly also how we bridge the technology into a policy message and what the relation is between those two.

DOT: One last question, what are your hopes or vision for the further development of the Internet?

KOLKMAN: I see fundamentally that this comes back to access and trust, and while those are the keywords of the Internet Society, they are also my words. I think it’s incredibly important that anybody who wants to have access to the Internet can get access to the Internet. No matter where you live, what race, what color, political background, which nation state, whether you live on an island in the Pacific, whether you’re visually impaired. To put it another way, I would like to see the last billion connected. That’s very important. But I also want to do that in a way that provides them with protection from harm that the Internet could bring to them. A reasonable certainty that if you do business, your identity won’t be stolen. A reasonable certainty that your private details are not harvested in aggressive ways. A reasonable certainty that things work as you should expect. So, trust. Really trust. Based on technical means, so that you can have some certainty that the trust is not based on a perception, but actually on a technical foundation.

Listen to this interview online at: https://www.dotmagazine.online/issues/who-rules-the-internet/Internet-keyholder
DNS, the keys to the Internet, and staking a territorial claim: An introduction to the Internet’s Domain Name System: How important it is, the elaborate security protecting it, and how companies can profit from using it well

It’s like a scene out of a Dan Brown novel – seven levels of security, to be accessed simultaneously by seven different individuals, recorded in detail and streamed live for auditing. Any false move may cause a time-out, which leaves those individuals locked in security cages. Armed guards standing watch.

Seven keys to seven safety deposit boxes in seven different rooms. Each safety deposit box containing a smart card in a tamper evident bag. Each smart card, a portion of the cryptographic key that protects the integrity of a central computer function.

Access to world-ending weaponry? No – access to the Internet. This is the Key Signing Ceremony, an elaborate ritual performed four times a year on fundamental Internet infrastructure. (For a first-hand description of the security involved in the Key Signing Ceremony, see A Day in the Life of a Man with a Key to the Internet, this volume, pg. 28)

All this carefully constructed security is in place to authenticate the Domain Name System, the largest and most widely-distributed database on the planet (http://www.linuxhotel.de/course/bind/), and a central – utterly essential – tool for the functioning of the Internet. Every single time you sit down at your laptop or on your smart phone and surf the Internet, each request you make in your browser for a particular website (be that via a link in another website or a URL that you type in manually), your computer needs to request information from the Domain Name System to find the location of the web server where that website is hosted, so that it can then contact that web server and provide you with the information you want.

The common metaphor for the Domain Name System is that it’s like a massive global telephone book. Instead of connecting people’s names with addresses and telephone numbers, the DNS connects the domain name of a website...
The root zone is a highly distributed and redundant set of name servers which contains all the information relating to the location of top-level domains (TLDs). So it would be the first port of call for your DNS resolver (the machine in your network that actually does the searching for you) when you send out a look-up query to find a website. The root zone points your resolver in the direction of the appropriate TLD names server (in our case, giving us the IP address for the .online name server), which in turn has information about the second-level domains (where to find dotmagazine.online).

This to-ing and fro-ing between different name servers to return the IP address we need takes place in a matter of milliseconds – far less time than it would take me to recall my telephone number.

The root zone is a highly distributed and redundant set of name servers which contains all the information relating to the location of top-level domains (TLDs). So it would be the first port of call for your DNS resolver (the machine in your network that actually does the searching for you) when you send out a look-up query to find a website. The root zone points your resolver in the direction of the appropriate TLD names server (in our case, giving us the IP address for the .online name server), which in turn has information about the second-level domains (where to find dotmagazine.online). This to-ing and fro-ing between different name servers in order to return the IP address we need to access the website we want takes place in a matter of milliseconds – far less time than it would take me to recall the telephone number of my mobile phone.

Securing the DNS – enabling validation and trust

The Domain Name System needs to be technically trustworthy – you want to know that when you type www.mybank.com into your browser, you will actually be directed to your bank, and not to a spoof website where a man-in-the-middle (https://www.techopedia.com/definition/4018/man-in-the-middle-attack-mitm) can then harvest your account details and drain your funds. And this is where the seven keys in seven safety deposit boxes come in. The Domain Name System Security Extensions (DNSSEC for short) allows zones within the DNS to be digitally signed so that they can be authenticated. This means that you know that the information has not been tampered with, and that the results of the search are authentic. This prevents malicious attacks like DNS spoofing (https://en.wikipedia.org/wiki/DNS_spoofing), where your company domain name may be hijacked for the sending of spam under fake names, for example, or man-in-the-middle attacks.

DNSSEC was applied to the root zone in 2010, meaning that answers returned can be validated if your network’s DNS resolver is DNSSEC aware – so you can trust that the answer has not been manipulated. The majority of TLDs are signed and deploy DNSSEC – so far, so good. But unfortunately, that’s where the deployment grinds to a halt. The vast majority of second and third-level domains are not validated with DNSSEC. As Olaf Kolkman, Cryptographer and Root Zone Key Holder, comments, "In [many] parts of the world, the success rate of percolating and maintaining those signatures is not very high. So that answers the question of how well the DNS is secured: not very well, because there are not that many signatures around. And this is a point of concern. In the Internet, we sometimes find it hard for people to invest in the security of others, so to speak. And this is an investment. Creating signatures is really an investment for any of the entities that need to do it... I think that is an issue because this whole infrastructure – almost everything we do on the Internet – starts with a DNS query. Being able to validate that nobody tampered with that is, I think, an incredibly good thing."

Now, making sure that your company domain name is signed with DNSSEC is not something you are likely to take care of yourself – the responsibility for this lies with the registrar through which you register your domain. ICANN (the Internet Corporation of Assigned Names and Numbers) maintains a list of registrars that deploy DNSSEC and the TLDs that they do it for: https://www.icann.org/resources/pages/pages/deployment-2012-02-25-en.
WHO RULES THE INTERNET?

Claiming the namespace - company branding through domains

So the Domain Name System is an ingenious system which saves us a lot of hassle and confusion online. But wait, there's more: Marketers should be clear that a domain name is a very powerful marketing tool for a company or a brand. Companies have several options for securing their namespace online. One of these is to purchase the same second-level domain with a wide range of TLDs (not just with a .com, but also .biz, .net, and any number of a whole range of new generic TLDs that have come onto the market in the last couple of years (https://www.icann.org/resources/pages/tlds-2012-02-25-en). This means that you can fill the namespace and have your company name under your control throughout the web.

The wonderful thing about domain names is that they are memorable, and the new TLDs give you the chance to make your website domain stand out even more.

But with the new generic TLDs, you can also be selective and clever in your choices. This means that you can find highly memorable, appropriate TLDs that add relevance to your domain name (dotmagazine is an online magazine, so dotmagazine.online works nicely, but your sports club might like to have a .club domain, your online shop a .shop domain, and so on). Another option is giving your domain name geographical relevance – if your company is a local company based in New York, for example, what about using .nyc as an option (see Mapping Virtual Space to the Geographical Environment – The Growth and Management of New geoTLDs this volume, pg. 40 for more information). The wonderful thing about domain names is that they are memorable, and the new TLDs give you the chance to make your website domain stand out even more.

Another option that companies have is to apply directly to ICANN (it is unclear at this stage when the next round of applications will be opened) to register your brand as an independent top-level domain – as Barclay's Bank did with .barclays & .barclaycard. As well as being memorable, the bank notes that "In the long term, the move will also add an extra layer of security for customers and clients as only Barclays and Barclaycard will be able to set up websites ending in .barclays and .barclaycard." (http://www.newsroom.barclays.com/fr/31622/uk_banking_first__barclays_launches_unique_branded_domain)

For companies and brands, there are also further initiatives to help with the growing potential of the new TLDs, like the Trademark Clearing House (TMCH, http://www.trademark-clearinghouse.com/) and industry initiatives like the Domains Protected Marks List (DPML, http://www.donuts.domains/services/dpml/dpml-overview) offered by Donuts.

Acceptance of new gTLDs

"Although it is now possible to have domain names and email addresses in non-Latin characters, such as in the Cyrillic, Hangul, Thai, Arabic, Hebrew, and Greek alphabets, the majority of Internet applications and systems still do not support them."

With the wealth of potential for the new gTLDs to open up opportunities for companies in their naming and marketing messages, another step is also important: Making sure that all systems are updated to be ready for new, longer top-level domains, and for new internationalized TLDs in a range of non-Latin alphabets. Systems architects and developers can find information here (https://international.eco.de/2016/news/introduction-to-universal-acceptance-published.html) on how to ensure that browsers, website logins, email clients, discussion forums, and so on are ready for what ICANN has dubbed "Universal Acceptance". To achieve Universal Acceptance, Internet applications and systems must treat all TLDs in a consistent manner, including new gTLDs and internationalized TLDs. Specifically, they must accept, validate, store, process and display all domain names.

"Although it is now possible to have domain names and email addresses in non-Latin characters, such as in the Cyrillic, Hangul, Thai, Arabic, Hebrew, and Greek alphabets, the majority of Internet applications and systems still do not support them," is the criticism of Lars Steffen, from eco – Association of the Internet Industry, and also Community Outreach Co-Coordinator for the Universal Acceptance Steering Group (UASG) at ICANN.

ICANN's multi-stakeholder approach as model for global governance

The Internet is a distributed, borderless conglomeration of autonomous networks – with root zone servers and name servers, data centers, and fiber backbone spanning the globe and falling under the auspices of multiple governments and a whole array of corporations and operators. So really it is fair to ask "Who Rules the Internet?" (see WHO RULES THE INTERNET? for more information, this volume, pg. ??). In the process leading up to becoming independent of the US government in 2016, ICANN developed a model of
governance based on the multi-stakeholder approach – bringing together the technical community, the private sector, governments, academia, and civil society around the table to find consensus on the future operation of Internet administration outside of the control of any one government. Thomas Rickert (see A Quiet Global Revolution for more information, this volume, pg. ??), Director of the Names & Numbers Forum in the eco Association and Co-Chair of the Cross Community Working Group on Enhancing ICANN Accountability, describes the process of developing this model and its remarkable effectiveness in building democratic consensus – and sees here a model for tackling many of today’s global challenges by ensuring widespread representation of the interests of the many stakeholders involved in these issues.

Judith Ellis

Read the article online here: https://dotmagazine.online/issues/who-rules-the-internet/claiming-and-protecting-virtual-namespace

THE DOMAIN NAME SYSTEM – MAKING A COMPANY WEBSITE FINDABLE

Sven-Holger Wabnitz, Visionary & Advisor

Sven-Holger Wabnitz explains how DNS works and how important it is for findability and brand identity in the Internet.

When companies develop an online presence, the first marketing thought is often website design. But taking a look at the deeper infrastructure has enormous benefits for not only brand identity, but also for brand protection. Understanding the opportunities that the Domain Name System offers is central to a strong online brand. eco’s Lars Steffen spoke to DNS pioneer Sven-Holger Wabnitz on behalf of dotmagazine about findability, security and brands in the DNS.

DOTMAGAZINE: Can you explain the idea of the DNS in a few words?

SVEN-HOLGER WABNITZ: You can compare the DNS with a phonebook and yellow pages, in which names of people and companies are mapped to telephone numbers, resources and services. You usually know the name of a person, but perhaps not his mobile number, so you use your phonebook.

The following example demonstrates this: if you want to visit the homepage of eco you just type into your browser www.eco.de instead of currently 178.77.101.60 or even much more complicated number-letter combinations with IPv6.

There are many more use cases out there for the DNS:

• When you send an email, the sending host needs the DNS to find the mail exchanger for the receiving domain.
• If you have a data centre and you have to change an IP number, you can just change it and the name stays (for example, the host on which the http demon www.eco.de is operated has to be changed and thus the IP number: visitors still type in www.eco.de).
• The management of the IP numbers: the so-called reverse IP management, which is basically a mapping from IP numbers to hosts.
• The DNS is also used in the context of VoIP, in supply chain management (RFID), especially in the Internet of Things (everything) area. Again: think of remembering of billions of IP numbers instead of simple names like: webcam.meetingroom1.cologne.eco.de.

The DNS is the backbone of the Internet; without it, the Internet would simply not function]

DOT: That sounds like a quite complex infrastructure. Can you explain the technical background to us in layman’s terms?
WABNITZ: Yes, you are right Lars, the DNS is a complex infrastructure. Let me give you a basic explanation without going into too many details. The DNS is the backbone of the Internet; without it, the Internet would simply not function. The DNS is a hierarchical distributed database, the root level is called “the root” which is operated by ICANN, the Internet Corporation for Assigned Names and Numbers. Each level in that hierarchy has its own authority which was delegated by its parent (e.g. eco.de.). Each node in that tree is called “zone”. Usually each of the delegated zones is operated on different servers (the name servers) than its parent. In each zone, there are database entries: information about sub-delegations of an authority and the mapping from names to resources of a specific type for example: the hosts IP address of www.eco.de.

DOT: That makes sense. I have one last technical question before we come to the importance of the DNS for companies: How does a workstation / desktop computer know which database instance to ask? What is the background to this?

WABNITZ: That’s a very good question, Lars. The infrastructure I described is called the authoritative DNS. Each of the name servers is responsible for the database entries it holds for a delegated zone including sub-delegations. But how do you find them? A delegated zone does not have any information about its parent. If you want to resolve a host name you have to start from the root and you basically say: dear root name servers, which name servers operate your child label “de”? After getting this answer, those name servers are asked which name servers operate the delegated label “eco” (which is concatenated to eco.de.). At the end, these name servers are asked for the entry of www.eco.de. The answer will be an IP number. Your browser now can connect to that IP number and ask the http service for the webpages of www.eco.de. But how can you find the root? Well, these name servers are well known worldwide by their IP number.

This task is called name resolution and is done by so-called resolvers or caching resolvers (caching because they remember the answers for a specific length of time to save traffic and speed up the resolving process). The resolvers are configured in your computer and you find it via the IP configuration “resolver” or “DNS server”.

DOT: We have all heard about the new top-level domains which are on the level one of the DNS hierarchy and operated by registries. Do you have any statistical data about the domain names and why domain names are important for a company?

In the end, it is all about brands and identification – no matter whether we speak about a private person, small, medium or large enterprises, organisations or governments.

WABNITZ: In the end, it is all about brands and identification – no matter whether we speak about a private person, small and medium companies, large enterprises, organisations or governments. Especially large enterprises own usually many brands and trademarks worldwide. They protect their brands against phishing, brand breaching and brand squatting through so-called defensive registrations: these companies register domains representing their brands and domains with typos under many country code top-level domains as well as new generic top-level domains.

They have a portfolio of hundreds, thousands or sometimes tens of thousands of domains and thus they have to care about internal processes and data related to those domains as well as everything related to finance and cost centres.

Assuming an average cost of $15 per domain per year, we are talking about a 5.01 billion dollar yearly revenue, growing at over 12% each year, not to speak of the reseller chain.

The new top-level domains have been launched for several reasons. One was for sure that the space of available names became thin but the demand for new names was still there. Let us take a look at some statistics out of the industry: there are over 334 million domains registered worldwide (status 2016). Since the beginning of the launch of the new TLDs (which is still ongoing), we can see still an increasing growth rate. We still have a growth rate of over 12.9% per year. Assuming an average cost of $15 per domain per year, we are talking about a 5.01 billion dollar yearly revenue, growing at over 12% each year, not to speak of the reseller chain. These numbers do not take into account emerging markets in underserved regions, which will be the markets of tomorrow. And domains are only the basis for the higher value services.

Carriers and the Internet industry have the responsibility to protect customer privacy.

WHO RULES THE INTERNET?
DOT: This sounds like we should pay attention to the DNS. Are there any regulatory rules or data privacy topics we should speak about?

WABNITZ: Yes, definitely. This is a very sensitive topic. At a first glance, you could say: well, the data in the DNS can be queried by anybody so the data is commonly available and there is nothing to protect. But looking behind the scenes: the operator of authoritative name servers and operators of resolvers collect the data of queries and can zoom into the data. They have the possibility to know who queries a certain domain and, in case of resolvers, they can evaluate which sites and services are used by a company. Today we all know the value of user tracking and profiling. Right at that point carriers and the Internet industry have the responsibility to protect customer privacy by keeping that information inside the country or a region. This is often the reason for a regulator to keep DNS servers inside the country or a specific region with similar data privacy laws.

DOT: This sounds like we should pay attention to the DNS. Are there any regulatory rules or data privacy topics we should speak about?

WABNITZ: An interesting question. It is very hard to attack the DNS because you need a lot of calculation power, bandwidth, and knowledge or a combination of these. There are basically diverse types of attacks, direct attacks and indirect attacks. We spoke earlier about the latter one: phishing, domain grabbing, and brand breaching.

The direct attacks can be divided into denial of service attacks and authenticity attacks. Let us speak first about the DDoS (distributed denial of service) attacks. As we already learned, the DNS is highly available thanks to the possibility of a distributed infrastructure. Anycast infrastructures make it even harder to attack the DNS in such a way. The side of the attacker needs either a massive bandwidth – which is nearly impossible to own because it is easy to find the source – or many devices with low bandwidth. And here we find the risk of the future. If somebody owns (here in the sense of a bot network) millions or tens of millions smart and small devices like cameras, routers, printers or any other – let’s call them IoT – devices, he can easily generate hundreds of millions of small / cheap queries to authoritative name servers. This will cause in an overload of the authoritative name server-infrastructure. As a result, zones hosted on those name servers will not be resolved any more (we exclude caching here). This happened a while ago with the name servers of the company Dyn (it was reported in media), which were attacked from tens of millions of IP addresses and as a result many more than 50 companies were not reachable anymore – including Amazon, Airbnb, CNN, Fox news, Netflix, Paypal, Twitter, and Spotify.

The other type of direct attacks, authenticity attacks, give the user wrong information. They are called DNS Spoofing and Cache Poisoning. One example: we all trust the so-called SSL secured data transfer via https. If we communicate via an https connection (we see the secure connections sign in the browser), we simply trust that connection and we think the data transfer is safe. But we cannot be sure who we are communicating with. The DNS resolver could have delivered a wrong IP number (remember: the web client needs the IP number of the webserver based on the DNS hostname) and our client connects to the wrong server which offers a SSL connection. You are simply redirected to another host / service. This can happen with ANY service. I believe I do not need to explain further consequences for the client and the company who offers the service. Such attacks are the mentioned and so-called “cache poisoning” attacks because the cache of a resolver is poisoned with false information. But there is solution in place which unfortunately is only used by the minority of companies / name servers / DNS hosters, and this solution is called DNSSEC. It increases security dramatically. DNSSEC ensures the integrity and authenticity of DNS queries. If done the authenticity is ensured up to the resolver of the provider (if you are a specialist up to the end of your own infrastructure). The connection between the provider running the resolver and the client is assumed to be secure. But it isn’t. There is a long way to go until an end-to-end authenticity is in place.
Each company should ask the questions: what is the cost per minute of Internet service failure or service redirection beside reputational damage.

The DNS as it is used today is only a proof of concept for much larger use cases in future.

Sven-Holger is an Internet pioneer and the inventor of the domain & DNS management software DomiNIC. His passions in the DNS area are disruptive use cases, DNS in the context of IoT, structural analysis, online brand protection as well as risk and security strategies.

Read the article online here: https://www.dotmagazine.online/issues/who-rules-the-internet/claiming-and-protecting-virtual-namespace/the-domain-name-system

The Growth and Management of New geoTLDs:
New geographical domain names allow companies, governments and individuals to identify their online presence with a certain regional community. Dirk Krischenowski, from dotBERLIN, explores how these are governed.

The introduction of new domain extensions (so-called top-level domains) like .berlin, .nyc or .swiss by the Internet’s administrative organization ICANN has been long awaited by cities, regions and language and cultural communities.

In 2013, for the first time in the history of the Internet, new top-level domains which correspond to the names of cities and regions were approved by ICANN. As a result, domain name registrars worldwide are offering Internet addresses in the eight German geographic endings .bayern, .berlin, .hamburg, .koeln / .cologne, .nrw, .ruhr and .saarland.

Germany is the pioneer and leader in the global development towards GeoTLDs and the world’s first publically available geographic domain extension, .berlin, came from Germany. ICANN expects dozens of other cities and regions from many other countries to follow this path and apply for their extension in the next 5-10 years.

All geographic top-level domains (GeoTLDs) have to get the permission of the relevant government(s) to operate the respective geographic string. The string could be the full name of a place (e.g. .sydney), a short form of the name (e.g. .rio), a common or official abbreviation (e.g. .bzh or .bcn), a translation to a foreign language (e.g. .cologne or .tokyo) or any other kind of association with the place name.

The operation of GeoTLDs by the Registry Operator, which is the organization that was contracted by ICANN to operate a GeoTLD, touches various areas of Internet governance. These areas are the subject of the paper “Mapping Virtual Space to the Geographical Environment” (Read the complete paper “GeoTLDs and Internet Governance” online, linked in the article: https://www.dotmagazine.online/issues/who-rules-the-internet/claiming-and-protecting-virtual-namespace/GeoTLDs)
GeoTLDs harnessed by the multi-stakeholder community

Following the successful introduction of the new geographic domain extensions, the first interim results indicate that their use by different local authorities follows different concepts of governance. While a few are governed more openly, like .com, and some are restricted, like .gov, the majority operate in a multi-stakeholder manner involving the local authorities, business associations, cultural groups, and citizens.

Comparing the domain registrations per inhabitants, those GeoTLDs that are merely operated by private organizations are more successful than those operated by the local government. This mirrors the experience in ccTLDs where business-driven extensions like .de have contributed much more to the country’s identity than those strongly influenced by the government like .fr or .it.

GeoTLDs in the context of digitization, smart city and e-government

GeoTLDs enable a significant improvement in the communication and findability of e-government services through Internet addresses which are brief and descriptive.

Meanwhile it is indisputable that new extensions have considerable potential for the communication of authorities with businesses and citizens in the context of digitization, smart city and e-government. They enable a significant improvement in the communication and findability of e-government services through Internet addresses which are brief and descriptive and which the target groups can very well remember (for example, www.gewerbeanmeldung.hamburg).

The new Internet addresses also provide a unified infrastructure for the digital connection of business and citizens to services of the administration and others, and can thus make an important contribution to improving the awareness and use of e-government services.

Some GeoTLDs

Want your own GeoTLD? Start planning now

Other cities and regions which are also interested in introducing their own domain ending have to be patient for the moment. ICANN has not yet set a specific timetable for a further round of applications. However, in view of the complexity inherent in the entire application procedure for a new domain ending, local authorities are well advised to discuss early on possible operating models and the financing possibilities for their own future domain ending.

Download the paper “Geo TLDs and Internet Governance” online here: https://www.dotmagazine.online/_Resources/Persistent/efc74e82194aaddea9757f71f7ca47126a9e97a/dot0317%204%20geo%20TLD%20paper.pdf

Read the article online here: https://www.dotmagazine.online/issues/who-rules-the-internet/claiming-and-protecting-virtual-namespace/GeoTLDs
Doing Business in Germany: Understanding Germany’s enthusiasm for Self-Regulation will make you want to get more involved.

In Germany, if your house is on fire, chances are that no professional firefighter will come to your aid. Instead, you’ll mostly rely on volunteers to respond to the scene and save your loved ones. Which works remarkably well: Volunteer firefighters may not be paid professionals, but they are experts nevertheless. In fact, the system works so well that the majority of the country’s almost 1.4 million firefighters are volunteers.

Volunteering is serious business in Germany, where one in four Germans is a part-time volunteer, mostly for social projects.

Volunteer firefighters are one of the logical results of a country made up of committed citizens who are used to taking care of things on their own.

What does this teach you about doing business in Germany?

In Germany, we like to
- get things done even before someone official says the word;
- get things done in a manner that prompts officials to seek our advice;
- get things done in a manner that negates the need for official solutions.
Get involved – and do expect involvement, especially from your customers.

These three approaches run deep in the country’s DNA and therefore in its industry, especially the Internet industry, which is why self-help and self-regulation have become such effective and efficient approaches. Should your company consider doing business in Germany, consider:

1. Getting involved. Extend your work beyond the borders of your organization. Join industry working groups, sit down with competitors to work on common standards and guidelines, use your expertise to advise officials at municipal, state and federal levels. Reach out to your customers and ask their opinions.

2. Expecting involvement – especially from your customers. They may think they can offer valuable contributions toward your business and know how to improve your products and services. Just as firefighters may not be professionals in the strict sense of the term, your customers might not appear on your payroll – but they just might be right.

Mathias Röckel

Read the article online here: https://dotmagazine.online/issues/who-rules-the-internet/DBIG-self-regulation

GMBH: EXCLUSIVENESS INCREASES VALUE

Marco Hoffmann from InterNetX explains the importance of the .gmbh top-level domain for gaining trust in the German market and doing business in Germany

DOTMAGAZINE: Who is eligible to register a .GMBH domain and why are there restrictions?

MARCO HOFFMANN: Domains with the extension .GMBH are reserved for companies operating as “Gesellschaft mit beschränkter Haftung” (limited liability companies). This opens up new and attractive possibilities for about 1.2 million GmbHs in Germany, Liechtenstein, Austria and Switzerland to present their businesses on the World Wide Web in the best way possible.

Registrants of .GMBH domains have to prove that they indeed are a GmbH, for example by providing an excerpt from the commercial register. This brings advantages for Internet users and companies alike. Companies benefit from the chance to present themselves under a unique seal of quality. For Internet users, the clear reference to the legal form in the domain name creates confidence at first glance and simplifies the communication between the company and Internet users. You can be sure that you are dealing with a real company.

The .GMBH registry itself (the entity that maintains the authoritative record of all registrations for the TLD) decided to limit the TLD to this group of clients, following regulations of the Internet Corporation for Assigned Names and Numbers (ICANN) and the Government Advisory Committee (GAC), among others. The GAC represents governments and governmental institutions in ICANN’s multi-stakeholder model and takes on an advisory role for the community.

DOT: Can you tell us something about the cooperation between different stakeholders? Were there any disputes and how were they resolved?

HOFFMANN: In hindsight, all parties involved – no matter whether we are talking about the chamber of industry and commerce, GmbH companies, registrars or applicants – had the same core requirements of a domain extension for GmbH companies, even though the specific motivations might have differed. ICANN’s multi-stakeholder model supported all interest groups and certainly contributed to making it easier for some to participate and stand up for their interests.
Basically, the focus is on Internet users and their expectations towards a website, i.e. the corresponding domain name. The domain extension allows a company, the registrant, to clearly identify itself as GmbH – much clearer than when using a .COM address, for example. In addition, it gives companies the opportunity to register their Internet address www.companyname.gmbh instead of companyname.de or companyname.com. This allows them to represent the whole company name in a short, catchy and self-explanatory domain.

SMEs in Germany consist almost exclusively of GmbHs and make up the backbone of the national economy - confidence in these companies has to be ensured.

Over the course of the ICANN new gTLD program, the commercial regulating authorities of the respective countries have become advocates for securing the interests of Internet users. The authorities were of course also aiming to prevent the misuse of the GmbH legal form and to protect the credibility of companies. This could have been the case had domain registrations under .GMBH not been regulated adequately. Small and medium-sized businesses in Germany consist almost exclusively of GmbHs and make up the backbone of the national economy. Confidence in these companies has to be ensured.

The Internet users decide whether or not they trust a website and if they want to do business with a company. Of course, this does not only depend on the domain name, but also on the content and design of the site. However, the domain name is the first thing you see (in ads, search results, flyers etc.), making it an important figurehead.

Finally, the parties involved agreed on so-called “safeguards” for certain sensitive strings. Besides .GMBH, other company extensions such as .SRL and .LTD (both abbreviations stand for limited liability companies, “SRL” mostly in Italy and Spanish-speaking countries and “Ltd” in English-speaking countries) are included in this list. As a registrar, the link between registrant and registry, we are taking on an important role in implementing the “safeguards” and are well aware of this responsible task.

DOT: Talking about self regulation and self governance: what are your experiences in the industry, especially in terms of .GMBH?

HOFFMANN: The new gTLD program and the introduction of .GMBH is an excellent example of ICANN’s multi-stakeholder model and as such an example for self-regulation and self-governance. Everybody could submit suggestions and together they tried to find a common denominator.

Although this process has proven to be lengthy and sometimes difficult, we have still had good experiences. The safeguards we have already mentioned are one example of a constructive community effort, since this is not a rigid construct, but still gives the implementing parties the freedom to adjust the execution to their respective business models.

DOT: With your background, how would you improve Internet governance, especially in terms of the domain industry?

HOFFMANN: The biggest challenges in these processes have surely been the lengthiness and complexity of the domain subject as well as the language barrier. The disadvantage that comes with the multitude of different parties in a multi-stakeholder model is that decision-making processes take up relatively large amounts of time. From the beginning to the end, when a solution is finally found, there are many hearings of all parties. Bearing in mind that the work of the stakeholder groups is largely based on voluntary commitment. Particularly in this area there is definitely room for improvement, as it is getting constantly harder to find volunteers. The topic of domains and DNS can be very complex and technical. Support through guides or tutors could help facilitate the entry of newcomers into the business.

Another obstacle is certainly language. English as business language makes sense for stakeholders from all over the world. But when it comes to the details, it can be difficult for non-native speakers to get further involved. They feel intimidated and might be afraid or ashamed to embarrass themselves by having problems in understanding a topic entirely. It might help to create local working groups for certain topics and only translate the results into English or to have the results presented to the international peers by a team leader. This approach would also allow for more insight into local laws. Internet governance is still heavily influenced by a U.S. American point of view and sometimes neglects the cultural and legal differences in different countries.
In addition, we should not let the influence of the different governments get out of hand. In particular, the community was successful in completing the IANA Stewardship Transition in 2016 (see A Quiet Global Revolution for more information, this volume, pg. 22), meaning that the administration of the Internet is no longer in the hands of the U.S. government under the supervision of the National Telecommunications & Information Administration (NTIA).
eco, with more than 1,000 member companies, is the largest Internet industry association in Europe. Since 1995, we have been instrumental in the development of the Internet in Germany, fostering new technologies, infrastructures and markets, and forming framework conditions. In the Competence Network, many influential specialists and decision makers of the Internet industry are represented, and current and future Internet themes are driven forward.

Special eco services help to make the market more transparent for providers and users. Our seal of approval ensures quality standards; our consultations for members and our services for users provide support in questions of legality, security and youth protection.

As an association, one of our most important tasks is to represent the interests of our members in politics, and in national and international committees. As well as our headquarters in Cologne, we have our own office in the German capital Berlin, and are represented at all relevant political decision-making processes in Brussels.

eco is a founding member of EurolSPA, the umbrella organization for European Internet associations, eco also represents the German industry with a seat on the Council of the Generic Names Supporting Organization (GNSO) at ICANN, and is a driving force behind the Internet Governance Forum – in short: We are shaping the Internet.