RELATÓRIOS DNS.PT

ÍNDICE

ICANN

ICANN | 54
Dublin

18-22 OCTOBER 2015

RELATÓRIO DNS.PT

Introdução

A ICANN n.º 54 decorreu na capital da Irlanda, Dublin, na semana de 17 de outubro. Nesta mesma cidade decorreu no início de novembro o Web Summit, um dos mais importantes eventos mundiais na área da tecnologia, que, como é sabido, irá realizar-se já a partir de 2016 em Lisboa. A organização do evento deixou-nos dados curiosos: 2395 participantes; 2426 equipamentos (entre telemóveis, computadores, ipad's, etc) ligados em simultâneo à Internet; 258 horas de tradução para inglês, 89 horas para espanhol e 59 horas para português. Ainda no campo das curiosidades, uma possível nota para os fabricantes de equipamentos, já que a organização identificou que, em termos de sistemas operativos ligados, a Apple se destacou com 62%, seguida de sistemas Android com 23% e, por fim, Windows com apenas 15%.

Nota prévia para destacar o facto de nas últimas edições da ICANN os temas em debate irem muito para além das questões técnicas, para as quais sabemos estarem maioritariamente orientadas as competências desta organização, focalizando-se neste momento muito na área da propriedade intelectual, cibersegurança, e mesmo dos conteúdos. Não obstante este facto, Fadi Chehadé, presidente da ICANN desde 2012 e prestes a terminar o seu mandato (março de 2016), alertou na sessão de abertura para o facto da ICANN apenas ser responsável pela camada técnica dentro do ecossistema da Internet.

Responsabilidade e missão da ICANN

ONE WORLD, ONE INTERNET

WHAT DOES ICANN DO?

To reach any device or thing connected to the Internet, you (or your search engine) must know their address – a name or a number. That address must be unique, so you can reliably find and connect to other devices, things, or information sources no matter where you are in the world. That's how the tens of thousands of physical networks appear and operate as 'One Internet'.

In concert with the technical operating community, ICANN maintains and administers the registries containing these unique addresses across the world ensuring the security, stability, and integrity of One Internet where we can reliably find each other.

Community-Driven Global Policy Development

To keep pace with dynamic technologies and rapid innovation, ICANN facilitates an open, consensus-driven, multistakeholder policy development process that is run from the bottom up.

Multistakeholder Model

Civil Society & Internet Users, the Private Sector, National & International Organizations, Governments, Research, Academic and Technical Communities are all represented.

Competition & Choice

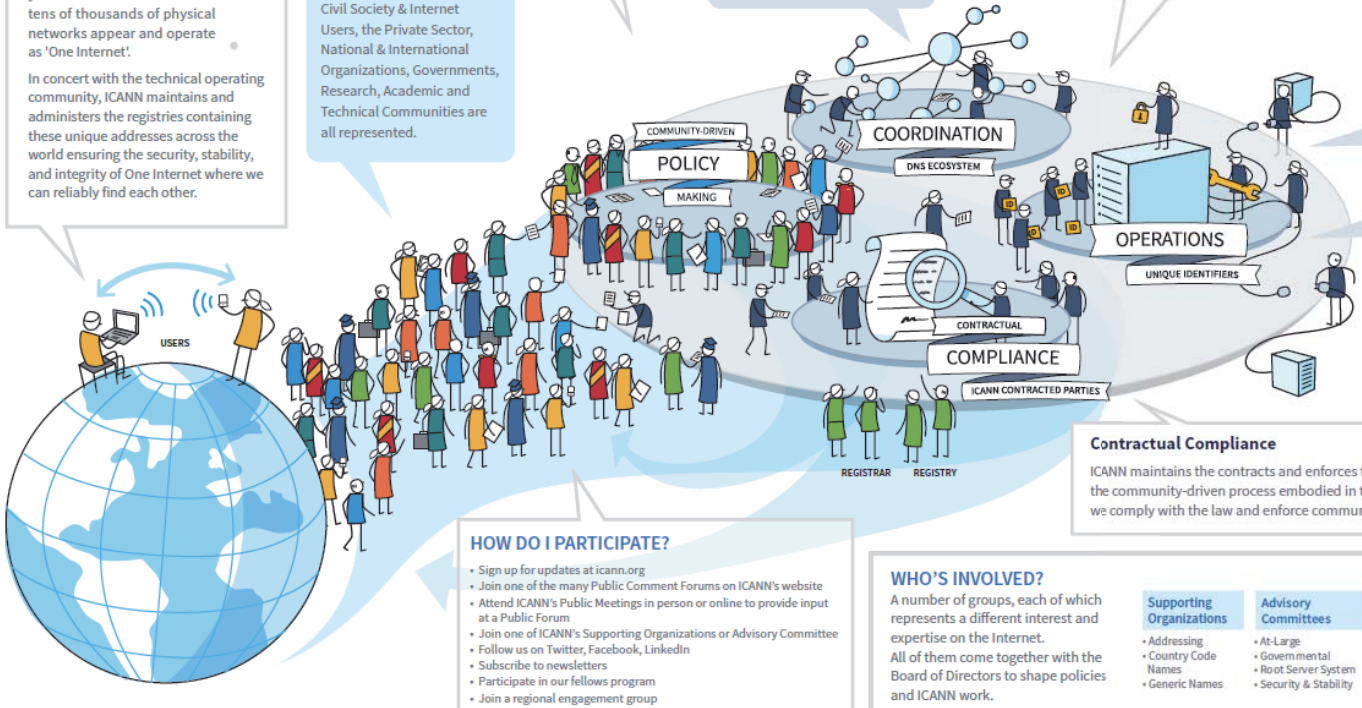
From accrediting over 1000 registrars, to introducing new Top Level Domains (TLDs), ICANN works to expand consumer choice by fostering competition and innovation in the domain name marketplace.

WHICH FUNCTIONS DOES ICANN COORDINATE?

DNS
- Development of generic TLD policy
- Facilitation of country code TLD policy discussions
- Delegation of and changes to Top-level domains
- Management of the root's DNSSEC trust anchor
- Facilitating Root Server System discussions

Internet Numbers
- Approval of global number allocation policies
- Allocation of top-level blocks of Internet numbers
- Recognize Regional Internet Registries

Protocol Parameters
- Creation of and changes to protocol parameter registries
- Management of the Time Zone Database



Security & Stability

ICANN supports DNS security by supporting a secured DNS infrastructure (DNSSEC) and managing the top-level key of that infrastructure, requiring close coordination and collaboration with the community and volunteers around the world.

Interoperability

ICANN's work plays a role in helping the community to develop new technologies that flourish while maintaining interoperability across the global Internet. For example, the central publication point of unique protocol identifiers maintained by ICANN makes it easier for protocol developers to create protocols that allow communications using secure connections between users.

Contractual Compliance

ICANN maintains the contracts and enforces the consensus policies developed through the community-driven process embodied in those contracts. While we are not a regulator, we comply with the law and enforce community policies through contractual obligations.

HOW DO I PARTICIPATE?

- Sign up for updates at icann.org
- Join one of the many Public Comment Forums on ICANN's website
- Attend ICANN's Public Meetings in person or online to provide input at a Public Forum
- Join one of ICANN's Supporting Organizations or Advisory Committee
- Follow us on Twitter, Facebook, LinkedIn
- Subscribe to newsletters
- Participate in our fellows program
- Join a regional engagement group

WHO'S INVOLVED?

A number of groups, each of which represents a different interest and expertise on the Internet.
All of them come together with the Board of Directors to shape policies and ICANN work.

Supporting Organizations
- Addressing
- Country Code Names
- Generic Names

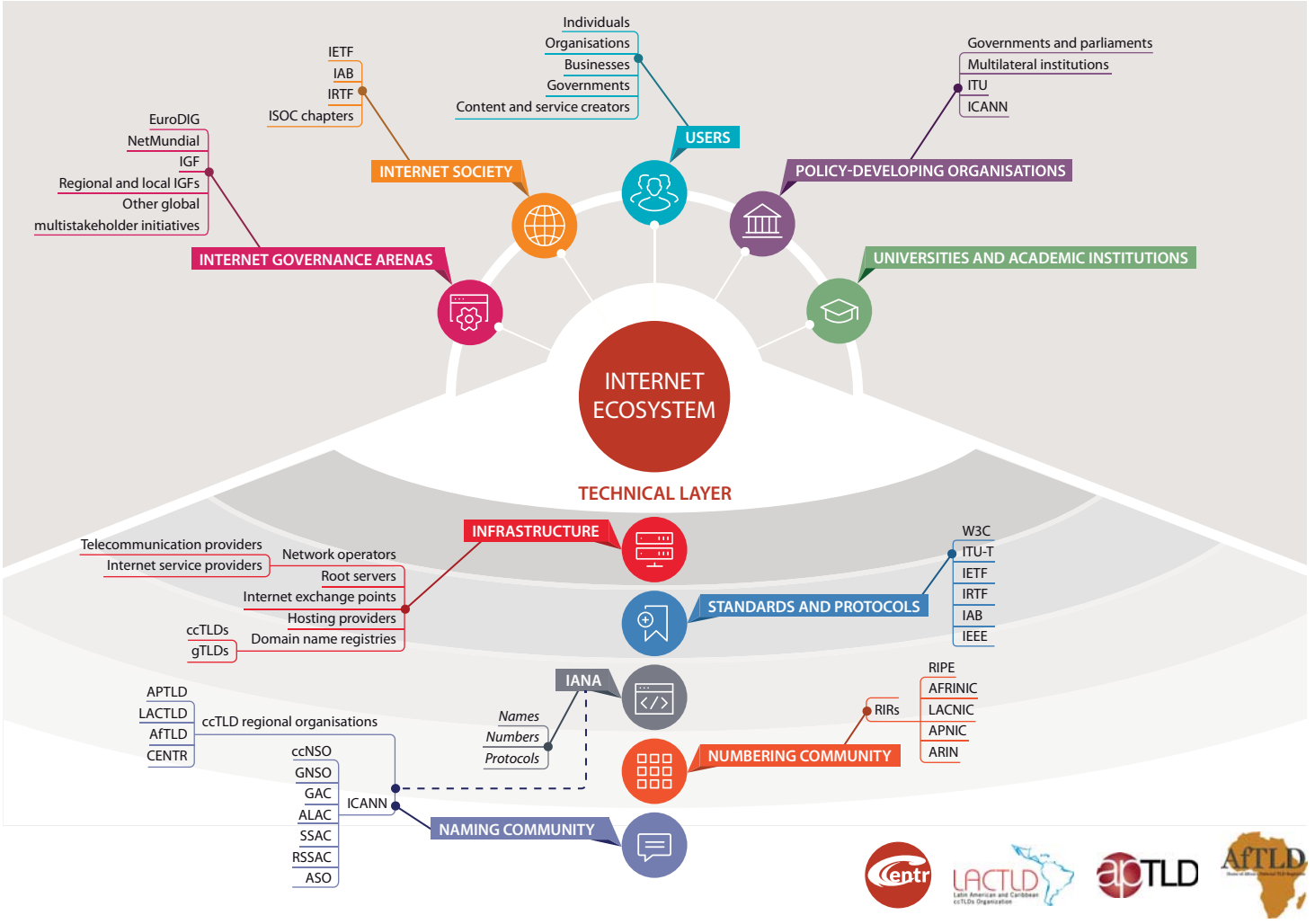
Advisory Committees
- At-Large
- Governmental
- Root Server System
- Security & Stability

Technical Advisory Bodies
- Technical Experts Group
- Technical Liaisons from IETF, ETSI, W3C, ITU

Board of Directors
- 16 Community Appointed Board Members

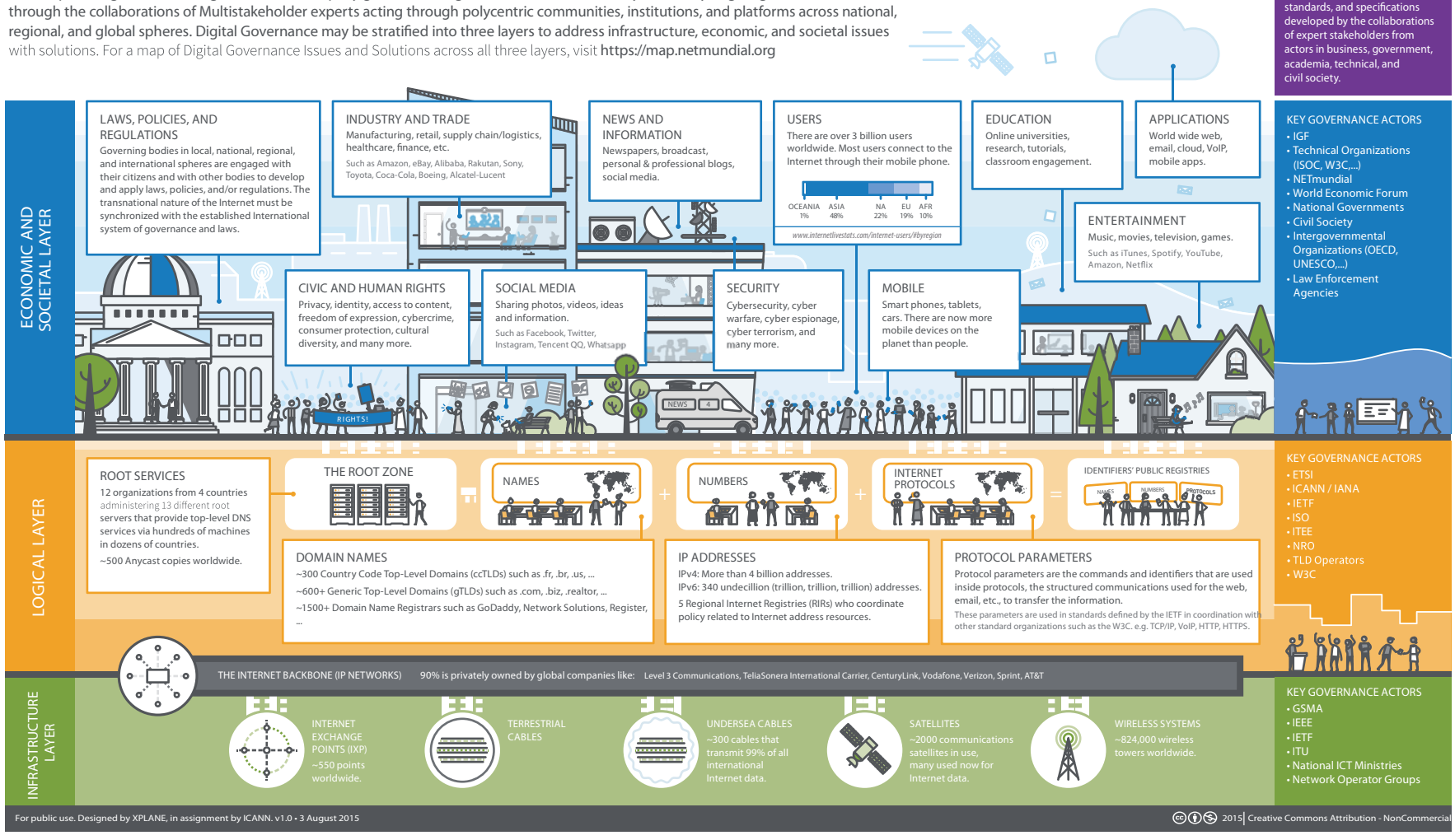
XPLANATIONS by XPLANE.com

Ecossistema da Internet



THE THREE LAYERS OF DIGITAL GOVERNANCE

No one person, government, organization, or company governs the digital infrastructure, economy, or society. Digital governance is achieved through the collaborations of Multistakeholder experts acting through polycentric communities, institutions, and platforms across national, regional, and global spheres. Digital Governance may be stratified into three layers to address infrastructure, economic, and societal issues with solutions. For a map of Digital Governance Issues and Solutions across all three layers, visit https://map.netmundial.org



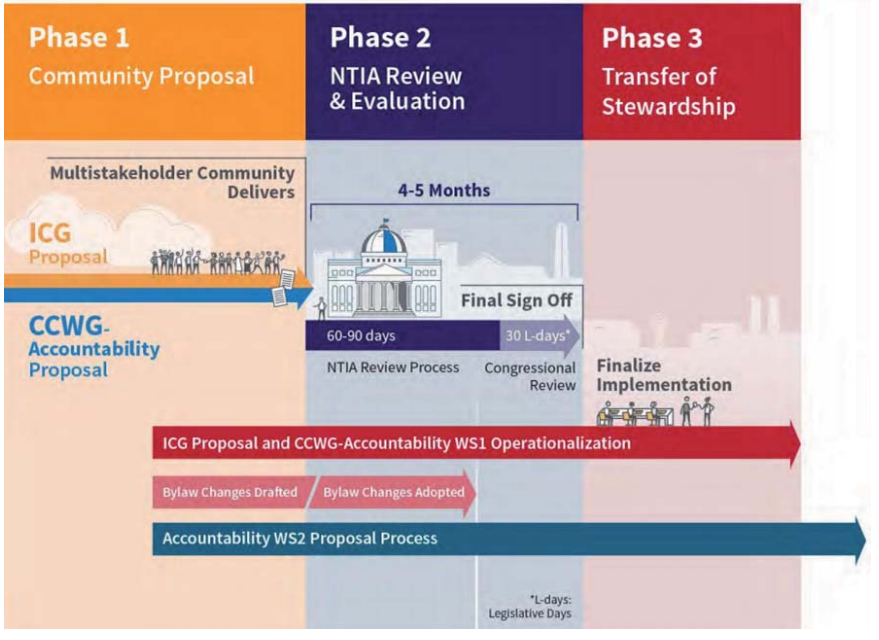
IANA Stewardship Transition[1]

Porém, ao longo dos quatro dias de trabalho o tema que monopolizou a discussão foi a transição das funções da IANA e a chamada accountability da ICANN, a que está associado o processo de prestação de contas e transparência de atuação desta entidade.

Acompanhámos em particular as cinco sessões organizadas pelo ccNSO (Country Code Name Supporting Organisation) a este respeito. Aqui a questão debatida foi a da responsabilidade do board[2], formas de nomeação dos seus membros e, mais relevante, possibilidade de recurso das decisões tomadas por este órgão cimeiro. A proposta do CWG (Cross Community Working Group) foi reiteradamente apoiada, embora se mantenham algumas pendências relevantes como seja o reajustamento dos estatutos que espelhem o novo modelo de organização da ICANN. Senão veja-se, a ICANN passará a não ter qualquer tipo de controlo por parte do governo Americano, ou outro, ou seja, matérias como a gestão do orçamento, a transparência das decisões, a forma de resolver questões associadas aos direitos humanos na Internet, a cibersegurança e a gestão pelos próprios governos em si pode ficar absolutamente fora de controlo e na dependência de uma entidade privada.

A proposta da CWG[3], que encerra os comentários e sugestões dos diferentes grupos de trabalho integrantes da estrutura da ICANN, já tinha sido aprovada na ICANN 53.º mas será agora objeto de novos reajustamentos.

Assim a calendarização de ações, a que já tínhamos feito menção, mantém-se, embora se antevejam já alguns atrasos:



1 https://www.icann.org/stewardship

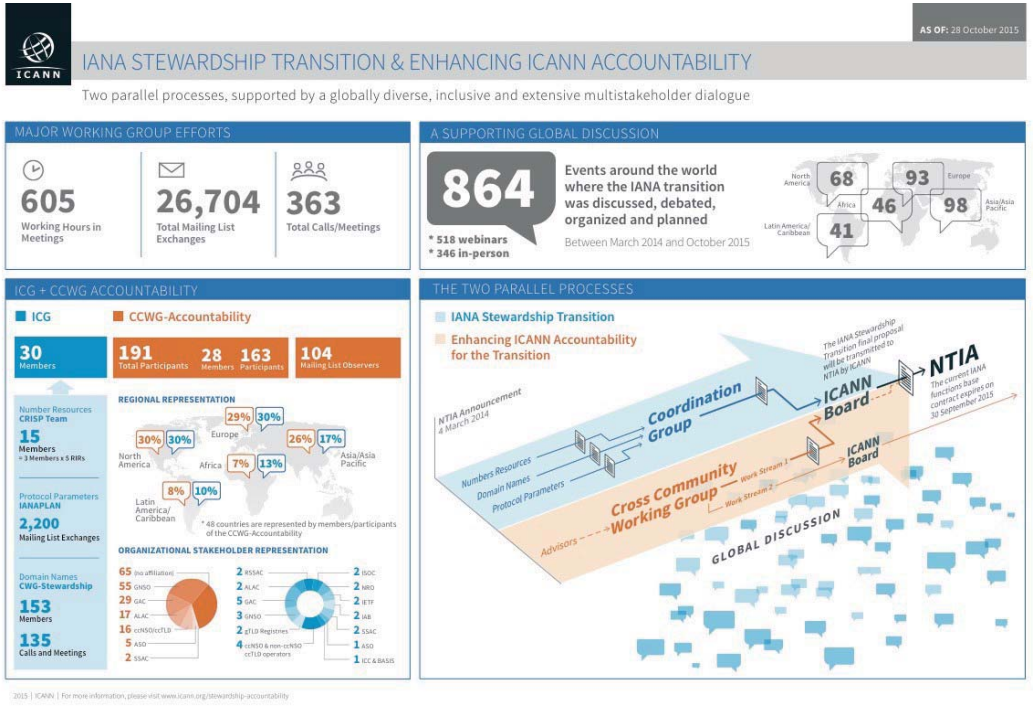
2 Chris Disspain, CEO do .AU (ccTLD Australiano) foi chair do ccNSO desde a sua criação em 2003, estando desde 2011 no board do ICANN como membro nomeado para fazer a ligação com os assuntos relativos aos ccTLD's.

3 CWG – Cross Community Working Group to Develop an IANA Stewardship Transition Proposal on Naming Related Functions.

Em resumo, neste momento estão ainda em discussão aberta, nomeadamente:

- Os novos estatutos da ICANN, com ampla participação da comunidade quer na redação quer na possibilidade de revisão futura;
- A definição de novos e específicos poderes para a comunidade ICANN que, designadamente, passem pela possibilidade de vetar orçamentos e documentos de gestão como sejam os planos de atividades anuais e possibilidade de destituição de membros do board;
- Um novo poder adicional que dá à comunidade voz ativa nas decisões sobre as revisões das funções da IANA, sendo que todos esses poderes da comunidade só podem ser exercidos depois de ampla discussão;

Será agora submetida a comentários uma terceira versão da proposta a submeter ao governo Americano.

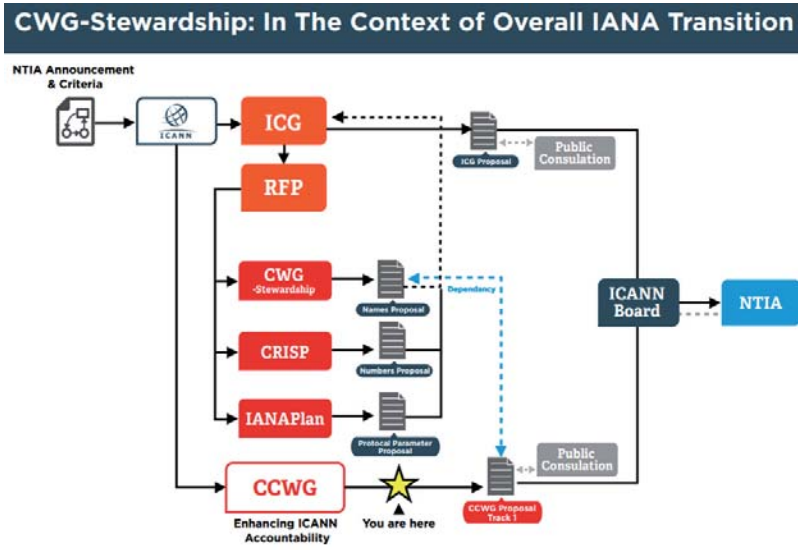


ccNSO

As reuniões do ccNSO (country code Names Supporting Organisation)[4] decorreram nos dias 20 e 21 de outubro, tendo, como dito acima e na senda do já passado na edição 53.º, o processo de transição das funções da IANA dominado os trabalhos, no entanto outros assuntos foram focados e deles faremos nota abaixo.

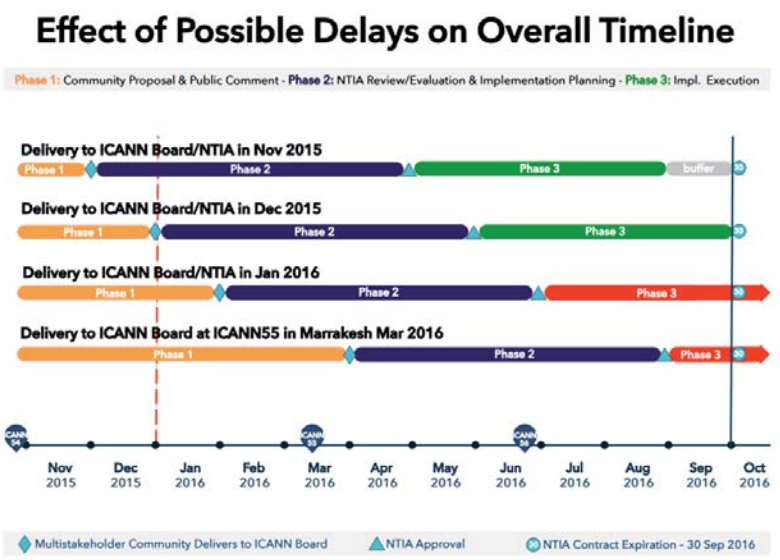
[4] O ccNSO foi criado em 2003, como grupo de trabalho que funciona junto do board do ICANN como representativo dos interesses dos ccTLD's, onde se inclui o .pt. É ainda uma plataforma de troca de conhecimento e boas práticas entre os congéneres de diferentes países.

Como é sabido o ccNSO está amplamente representado (cinco membros) no CCWGA, estando a participar ativamente na discussão das matérias relativas ao processo de transição das funções da IANA, a que está associada a questão da prestação de contas da ICANN, cujos pontos em aberto acima já fizemos nota. De qualquer forma, uma das questões que tem preocupado mais a comunidade técnica tem sido a Service Level Expectation da IANA, cujo âmbito e alcance deve continuar a ser obrigatoriamente garantido, já que tem a ver com questões relativas à manutenção da root zone com as características de segurança e confiabilidade que se impõem[5].



Neste fórum foram apontados especiais riscos decorrentes do atraso no processo como sejam a possibilidade da comunidade começar a dispersar e perder o interesse e credibilidade no processo, a possibilidade de, via revisão decorrente do WSIS, os governos tenderem a criar outra entidade para assumir as competências da IANA e, em última análise, começar a ser posto em causa o funcionamento e eficácia do modelo multistakeholder.

Possíveis efeitos dos atrasos na calendarização inicialmente fixada:



5 Veja-se: https://meetings.icann.org/en/dublin54/schedule/tue-ccnso-members/presentation-iana-sle-20oct15-en.pdf

Novos gTLD's

Olhando mais uma vez para os números, neste momento encontram-se delegados 795 novos gTLD's, fruto das 1930 candidaturas apresentadas. Foram entretanto retiradas 536 candidaturas e não aprovadas 37. No mês de novembro encontram-se já registados 10 milhões de domínios sob os novos gTLD's, sendo que cerca de 16% deste número refere-se a domínios registados sob .xyz (1.6 milhões) eem segundo lugar no ranking de registos vem o .top com cerca de 890 000 registos.

No leque da totalidade dos novos gTLD's os chamados geo gTLD's continuam a ter algum sucesso. No topo está o .nyc com perto de 87 500 registos, o .london com 70 600 e o .berlin com 68 300. Neste último caso, uma nota curiosa é o facto de a cada criança que nasce em Berlim ser-lhe atribuído um domínio .berlin. Entretanto o Rio de Janeiro foi a primeira cidade da América Latina a ter um gTLD. O .rio foi lançado no passado mês de setembro, pela Prefeitura do Rio de Janeiro embora seja gerido técnica e administrativamente pelo NIC.BR, na sequência de um contrato de concessão. Até novembro estavam registados cerca de 1000 domínios, com um custo unitário de cerca de 130 reais. Este registo implica o cumprimento de um conjunto de regras, sendo que a mais relevante é a necessidade do titular do domínio ter uma ligação (naturalidade e/ou residência) à cidade do Rio. Adicionalmente foi bloqueado um conjunto de nomes que não podem ser registados, referimo-nos a 92 cidades periféricas como sejam angradosreis.rio ou teresopolis.rio, ex-libris da cidade como paodeacucar.rio, corcovado.rio, etc.

À semelhança do já noticiado na edição anterior, no que respeita à utilização de códigos de países como domínios de segundo nível nos novos gTLD's, o GAC[6] continua a desenvolver uma base de dados de requisitos do país de notificação de pedidos de liberação de nomes de país[7]/território. Este trabalho quando estiver concluído será publicado no site do GAC[8]. A não aceitação do registo de domínios de topo (gTLD's) com duas letras continua a assentar em argumentos como a letra do RFC 1591 e nos standards passados já estabelecidos pelo ICANN e amplamente adotados mesmo fora do DNS[9].

Neste momento olha-se já um pouco para o futuro e antecipam-se algumas questões que podem vir a surgir na próxima ronda que a ICANN venha a abrir para registo de novos gTLD's. Inclusivamente, o GAC dirigiu ao board um pedido para esclarecer a comunidade sobre os problemas que têm sido detetados ao nível da existência de, por exemplo, condutas abusivas como malware, botnets, phishing, pharming, pirataria, violação de marcas e/ou direitos de autor, falsificação, práticas fraudulentas ou enganosas e outras atividades ilegais.

6 Governmental Advisory Committee (GAC). A recomendação anterior do GAC ao board neste campo foi no sentido de criar procedimentos e mecanismos em que os governos que não pretendam ver o código do seu país ou o respetivo nome utilizado para este efeito, tenham o seu direito salvaguardado sendo notificados obrigatoriamente sempre que haja um pedido nesse âmbito.

7 A Alemanha liberou completamente a utilização do .de como domínio de segundo nível para gTLD's, Portugal, como de resto grande parte dos países, tem tomado uma posição mais conservadora, protegendo o .pt, mas, em simultâneo, não fechando a possibilidade de revisão desta opção em função daquilo que venha a ser a evolução do mercado.

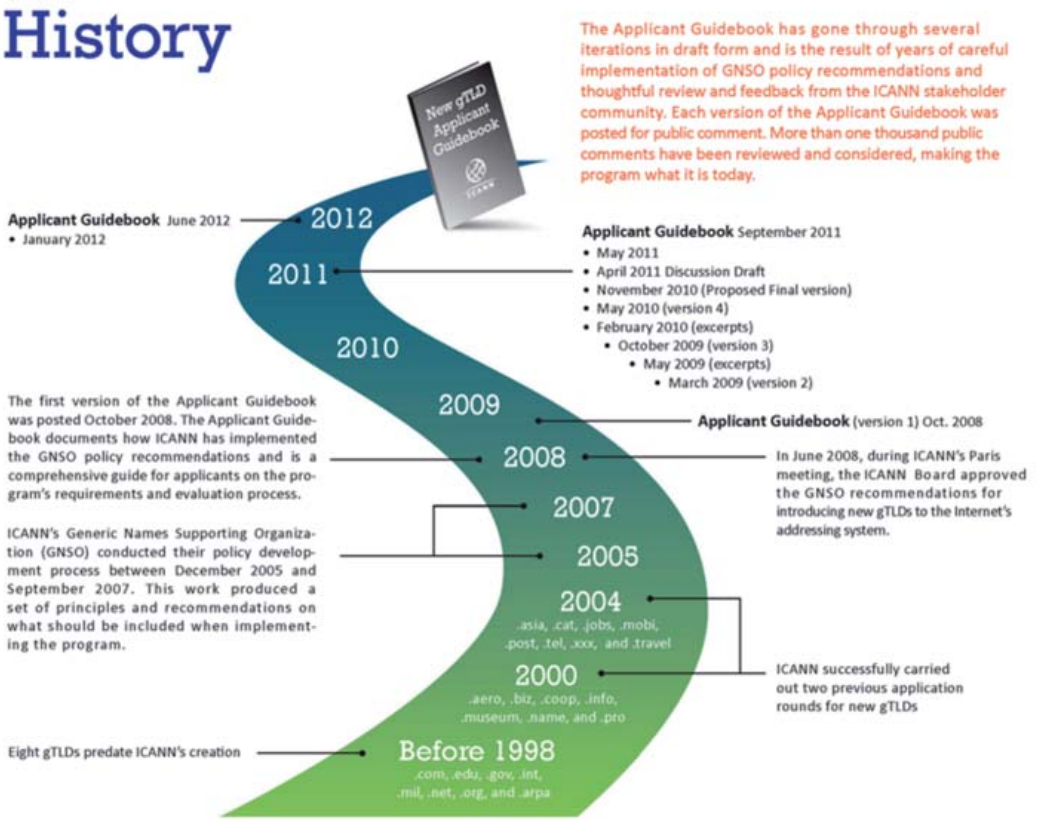
8 https://gacweb.icann.org/display/gacweb/Governmental+Advisory+Committee

9 https://www.icann.org/resources/pages/two-character-comments-consideration-2015-10-06-e

Uma questão mais concreta é a permissão do potencial uso futuro de mais de 300 códigos constantes na lista ISO 3166-1 alpha 3 (por exemplo PRT para Portugal). As opções na mesa são: permitir o seu registo como novos gTLD's desde que não conflituem com códigos de três letras de países, simplesmente não permitir o seu uso ou, terceira alternativa, permitir o seu uso só por ccTLD's. Entretanto o CENTR já lançou um survey à sua comunidade para aferir sobre a melhor opção a seguir. Prevêem-se já algumas decisões na reunião de março de 2016. Por fim, continua como premente a revisão dos termos e condições a que os registrars e os registries devem obedecer em matéria de WHOIS, desde logo para garantir mais confiança e fiabilidade nos dados associados a cada domínio. Esta será uma imposição que futuramente ficará plasmada numa perspetivável revisão do RAA (Registrar Accreditation Agreement).

Relembrando como tudo começou:

A segurança e as questões a ela associadas, quer seja na componente técnica quer no que respeita, em última análise, à proteção do consumidor são sempre um dos tópicos mais debatidos. Nesta edição decorreu uma sessão particularmente interessante sobre o problema com que a indústria farmacêutica se tem debatido na luta contra a venda ilícita de medicamentos online.
Sob pena de estarmos aqui a entrar na área dos conteúdos a verdade é que as conclusões foram unanimes no sentido de por um lado se impor o lançamento de campanhas de sensibilização generalizada e, por outro, ver envolvidos neste processo não só as farmacêuticas, mas também os registries, os registrars, os gestores de motores de busca, enfim todos os elos da cadeia de valores.



Foram-nos deixados números que se podem qualificar como assustadores, por exemplo, 97% das vendas online de medicamentos são ilegais e não autorizadas ou certificadas pelas entidades competentes, sendo que 62% dos medicamentos vendidos são falsificados o que constitui um problema de saúde pública. Até outubro de 2015, só nos EUA tinham sido encerrados 2410 sites de venda ilicita de medicamentos. Tratando-se de um problema global têm de ser encontradas soluções globais, nesse campo têm surgido iniciativas concertadas entre vários países como a PANGEA[10] que, inclusivamente, disponibilizam bases de dados completas de sites que comercializam legalmente medicamentos. Num mercado altamente regulado como este, o consumidor deve estar alerta, por exemplo, para o facto de lhe ser proporcionado o acesso a medicamentos com um custo muito mais baixo do que o praticado no mercado tradicional e sempre sem qualquer necessidade de prescrição médica.

O registry de .se, IIS, (ccTLD da Suécia) apresentou o caso em que se viu recentemente envolvido no âmbito do processo crime piratebay.se. Este site, como é sabido, disponibilizava livremente filmes, música e audio books sem autorização dos legítimos detentores de direitos. O que aconteceu na Suécia foi inédito já que o registry foi acusado de cumplicidade na violação de direitos de autor. A acusação vinha alegar haver uma conexão entre o domínio em causa e esta violação, sendo o domínio um instrumento para a comissão do crime. O ministério público litigou ainda que o registry tem plenos poderes sobre o domínio e nada fez, ou seja agiu de forma cúmplice, inclusivamente renovou o domínio e continuou a prestar o serviço. O registry, na contestação, veio alegar que só age depois de uma decisão do tribunal e que não faz análise de conteúdos. O tribunal absolveu o IIS, considerando que não havia obrigação por parte do registry de atuar no sentido de remover unilateralmente o domínio. Este processo é pois um reflexo claro da questão que hoje começa a ser debatida sobre o papel dos registries – como é em Portugal a Associação DNS.PT – na gestão e eventual supervisão dos conteúdos associados a cada domínio. Não é hoje claramente esse o papel dos registries.

10 http://www.interpol.int/Crime-areas/Pharmaceutical-crime/Operations/Operation-Pangea

Um outro caso que foi apresentado, e que aqui fazemos nota, foi o caso weinsteins&others vs Iran&others que remonta a 1997, na sequência de um ataque bombista que matou e feriu vários cidadãos amercicanos em Jerusalém, e onde os estados Iranianos e Sírios foram condenados a pagar uma indemnização civil às vítimas. O caso nasce na sequência da condenação destes estados, ou melhor na procura de bens – casas, obras de arte em museus americanos, etc - que possam de alguma forma satisfazer o valor indemnizatório que atinge vários milhões de dólares. A impossibilidade de encontrar bens capazes de satisfazer este montate levou a que a ICANN fosse chamada ao processo no sentido de serem penhorados os ccTLD's destes países. Nesta sede a ICANN veio invocar que os ccTLD's não são propriedade dos réus; ainda que sejam não são penhoráveis nem objeto de transferência nos termos solicitados, sendo que, aindaque sejam penhoráveis, a penhora não pode recair sobre a ICANN. A primeira sentença remonta já a outubro de 2014, tendo a ICANN sido absolvida com base no argumento de que um ccTLD não é penhorável [embora possa ser propriedade] já que só tem existência "(...) as they are made operational by the ccTLD managers." Os autores recorreram no passado mês de agosto invocando uma possível interpretação do D.C Code 16-544, segundo a qual nomes de domínio e endereços IP podiam ser configuráveis como bens penhoráveis. Aguarda-se decisão que, como no caso anterior, pode fazer doutrina.


ICANN | 54 • TECH DAY

Opening Remarks:
Eberhard Lisse

A habitual sessão "*Tech Day*" do ICANN ocorreu a 19 de outubro, imediatamente depois da sessão formal de abertura da conferência, e foi moderada por *Eberhard Lisse, chair do Technical Working Group* do *ccNSO*, e responsável do ccTLD .NA da Namíbia.

.VE Data Cleanup:
Rumary Ricaute

Rumary Ricaute da *Comisión Nacional de Telecomunicaciones (CONATEL)*, o *Registry* do ccTLD .VE da Venezuela, iniciou a sua apresentação com uma sequência cronológica de eventos importantes que ocorreram neste domínio de topo, desde da sua delegação em 1991. De destacar no âmbito da apresentação, o incidente em 2009, onde um vírus informático procedeu à criação indevida de mais de 40.000 domínios na base de dados de negócio, e o incidente em maio de 2012, onde a falha de hardware provocou um apagão generalizado da Internet em .VE, aproximadamente por 2 horas.

Na sequência destes incidentes, o .VE decidiu encetar um conjunto de iniciativas que visam aumentar a disponibilidade, a fiabilidade, a eficiência e a segurança de informação. Uma das iniciativas é o estudo da qualidade de dados, que segundo as previsões iniciais irá permitir a eliminação de 230.000 domínios, num universo aproximado de 320.000 à data de setembro de 2015. Os domínios a remover encontram-se em situação irregular, ou seja, associados a informação falsa, de titulares e pagamentos. Prevê-se que o processo de remoção ocorra durante 6 semanas. Com esta iniciativa o .VE espera um aumento de 20% na fiabilidade dos dados na respetiva base de dados de domínios.

A outra iniciativa foi a migração da plataforma de registo de domínios para uma nova solução mais robusta, que entre outros aspetos, permitiu melhorar a disponibilidade da página de registo de domínios .VE de 59% para 98%, e reduziu os tempos de resposta dos processos de registo.

Importa destacar, que a metodologia apresentada no processo de limpeza de dados pelo .VE é considerada agressiva, pouco comum na comunidade de ccTLD's, mas ao mesmo tempo apresenta uma grande eficácia.

Por ultimo, em resposta a uma questão da audiência sobre planos para implementar DNSSEC e RDAP, o .VE afirmou a intenção para implementar DNSSEC, provavelmente no segundo semestre de 2016, no entanto estão ainda a reunir conhecimento sobre essa matéria.

The ZoneMaster:
Wallström

Vincent Levigneron, do .FR da França e Patrik Wallström do .SE da Suécia, apresentaram a ferramenta ZoneMaster, uma aplicação para avaliar tecnicamente delegações DNS. Trata-se duma iniciativa conjunta entre a AFNIC e IIS o Registry do .SE. Este projeto iniciou em outubro de 2013, atualmente a aplicação encontra-se sólida e estável.

É uma aplicação open source projetada para ser o "estado de arte" das ferramentas de avaliação de nomes, escrita de raiz em Perl, com um conjunto verdadeiramente vasto de funcionalidades. Vincent Levigneron apresentou o projeto e por último procurou envolver a audiência, fazendo um apelo aos contributos da comunidade, nomeadamente através do uso da aplicação, a deteção e o relato de bugs, sugestões ou melhorias. Patrik Wallström fez uma apresentação do ponto de vista operacional, com alguns exemplos de utilização prática da solução, e referiu ainda trabalhos que se encontram em curso, nomeadamente o suporte para múltiplos perfis de avaliação, suporte para domínios com caracteres IDN.

The New .CL:
Urzúa

José Urzúa, do .CL do Chile apresentou o projeto "Novo .CL", iniciado em 2013 teve como objetivo adotar um novo regulamento de registo de domínios e um novo sistema de informação, mais

adequado às necessidades do serviço atuais deste ccTLD.

Alguns dados do ccTLD .CL, foi delegado em 1987 mas só se tornou operacional 6 anos depois em 1993, tal como o .PT em 2005 disponibilizou o suporte para domínios com caracteres especiais IDN, tem suporte para IPv6 desde 2007 e DNSSEC desde 2011, e atualmente conta com mais de 500.000 domínios registados.

O novo sistema de informação foi desenhado e desenvolvido internamente pelo .CL à medida das suas necessidades, é um sistema de 3 camadas (frontend, aplicacional e base de dados). Este sistema entrou em produção em novembro de 2013, mas o .CL optou por manter ambos os sistemas de informação, novo e antigo em execução, como dois registrars internos, o sistema antigo só será descontinuado quando todos os domínios forem geridos pelo novo sistema. O .CL afirmou ainda que está a trabalhar na funcionalidade que lhe irá permitir a existência de entidades registrars externas à organização.

Host Presentation:
Steven Farrell

Steven Farrell do .IE da Irlanda, apresentou a iniciativa "IEncrypt" desenvolvida em conjunto com a empresa Tolerant Networks Limited. Trata-se de uma iniciativa que procura estimular a utilização de canais de comunicação encriptados na Internet.

Segundo a observação do tráfego Internet dos últimos 20 anos, apenas 30% de páginas na Internet utilizam SSL, sobretudo em páginas de empresas de pequena dimensão, quer seja por uma questão de falta de recursos, desconhecimento ou até desvalorização. Esta situação favorece o desenvolvimento de atividades maliciosas, com custos avultados para todos, empresas e utilizadores.

Com esta iniciativa a adoção de DNSSEC e de certificados SSL é imediata, desde do primeiro momento de criação do domínio, simplesmente através de uma checkbox.

Numa primeira fase, já foi feita uma demonstração do conceito funcional, nas fases seguintes serão encetados esforços para implementar em produção. A intenção é de disponibilizar a solução à comunidade sobre o enquadramento open-source com licenças BSD.

TLD Data Analysis:
Wullink

Maarten Wullink, do .nl apresentou um resumo dos trabalhos desenvolvidos no âmbito de soluções para análise de dados DNS de um domínio de topo (TLD). É muito comum um TLD gerar conjuntos de dados com características de "Big Data", no decorrer da sua atividade, em particular quando se incluí o trafego DNS.

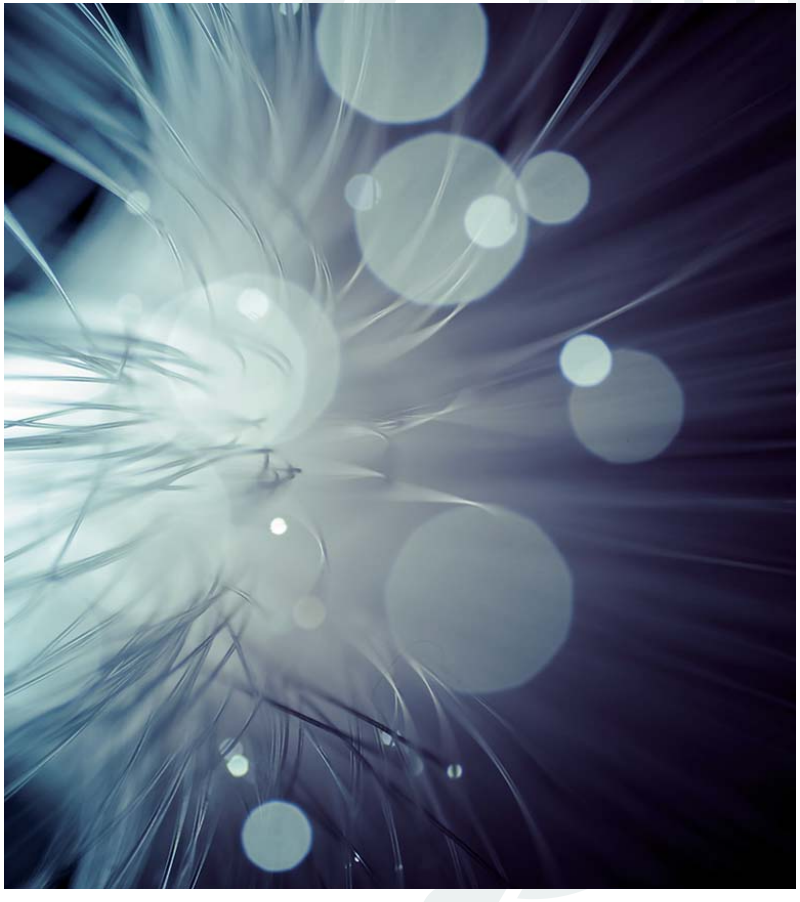
A análise e o tratamento destes dados são portanto um desafio para o qual não existe uma solução simples e eficaz. Assim o .NL encetou um projeto de análise e chegou a conclusão que a melhor resposta para este desafio, é a seguinte combinação de aplicações: Hadoop HDFS, Parquet e Impala.

A solução encontrada irá permitir o reforço das iniciativas de segurança, nomeadamente a identificação de domínios utilizados em atividades maliciosas e botnets, assim como projetos do próprio .NL e universidades.

Reputation Metrics Design:
Korczyński

Maciej Korczyński da Universidade de Tecnologia de Delft na Holanda apresentou a iniciativa REMEDI3S-TLD, desenvolvida em colaboração com o SIDN, o Registry do .NL.

Trata-se de uma iniciativa que procura estabelecer um conjunto de métricas de reputação de segurança, com base nas características especificas do ecossistema DNS e nos incidentes de segurança existentes, para melhorar o nível de segurança da Internet em termos nacionais e nos TLDs em geral.



Early Domain Names:
Arends

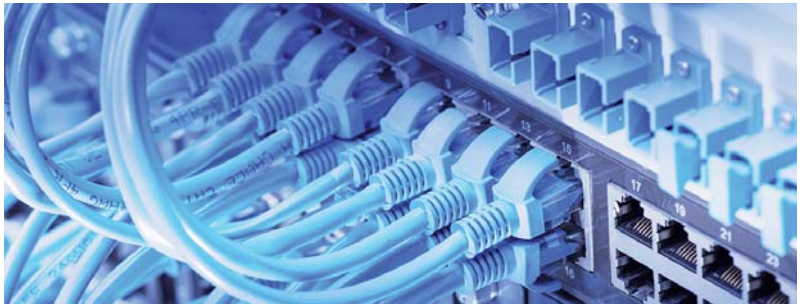
Roy Arends, do ICANN, antigo colaborador da Nominet o Registry do .UK do Reino Unido, levou a audiência presente numa viagem ao passado, ao apresentar os resultados da sua pesquisa pelos primeiros domínios existentes, ou o quem mais se aproxima do conceito atual de domínio.

A história de nomes recua a setembro de 1969 na Universidade da Califórnia, quando foram trocadas as primeiras mensagens entre 2 sistemas, na ARPANET. Este momento é considerado por muitos a origem da Internet atual.

Em 1973 surgiu a primeira solução de nomes centralizada, gerida pelo instituto de pesquisa de Stanford (SRI-NIC), ainda com recurso ao conhecido ficheiro hosts, partilhado por FTP e mais tarde pelo serviço de nomes no porto 101.

Ainda em 1973 com apenas 40 pontos de acesso e 48 sistemas surgiram os primeiros problemas de escala, devido elevado número sistemas ligados, uma década depois em 1983 a rede já comportava 5.500 pontos de acesso

De realçar que grande parte dos intervenientes iniciais desta história, como Vint Cerf e Steve Crocker ainda se encontram entre nós, muitos deles ativos na comunidade Internet.



RDAP Authentication:
Scot Hollenbeck

Scot Hollenbeck da Verisign apresentou a solução de autenticação federada para RDAP da Verisign. RDAP é um protocolo apontado como sucessor do serviço Whois, com um vasto conjunto de funcionalidades, nomeadamente de controlo de acesso à informação.

Para garantir essas funcionalidades o protocolo RDAP necessita de identificar e autorizar os clientes que procuram a informação relativa a domínios. No entanto o modelo tradicional de autenticação cliente/servidor pode não ser o mais adequado, devido a problemas de escalabilidade, à medida que a adoção do protocolo RDAP é mais comum. Assim surgiu a solução de autenticação federada, que permite a utilização de uma única credencial para aceder a múltiplos servidores de RDAP.

A solução em estudo pela Verisign utiliza os standards OpenID, OAuth e está em fase de protótipo.

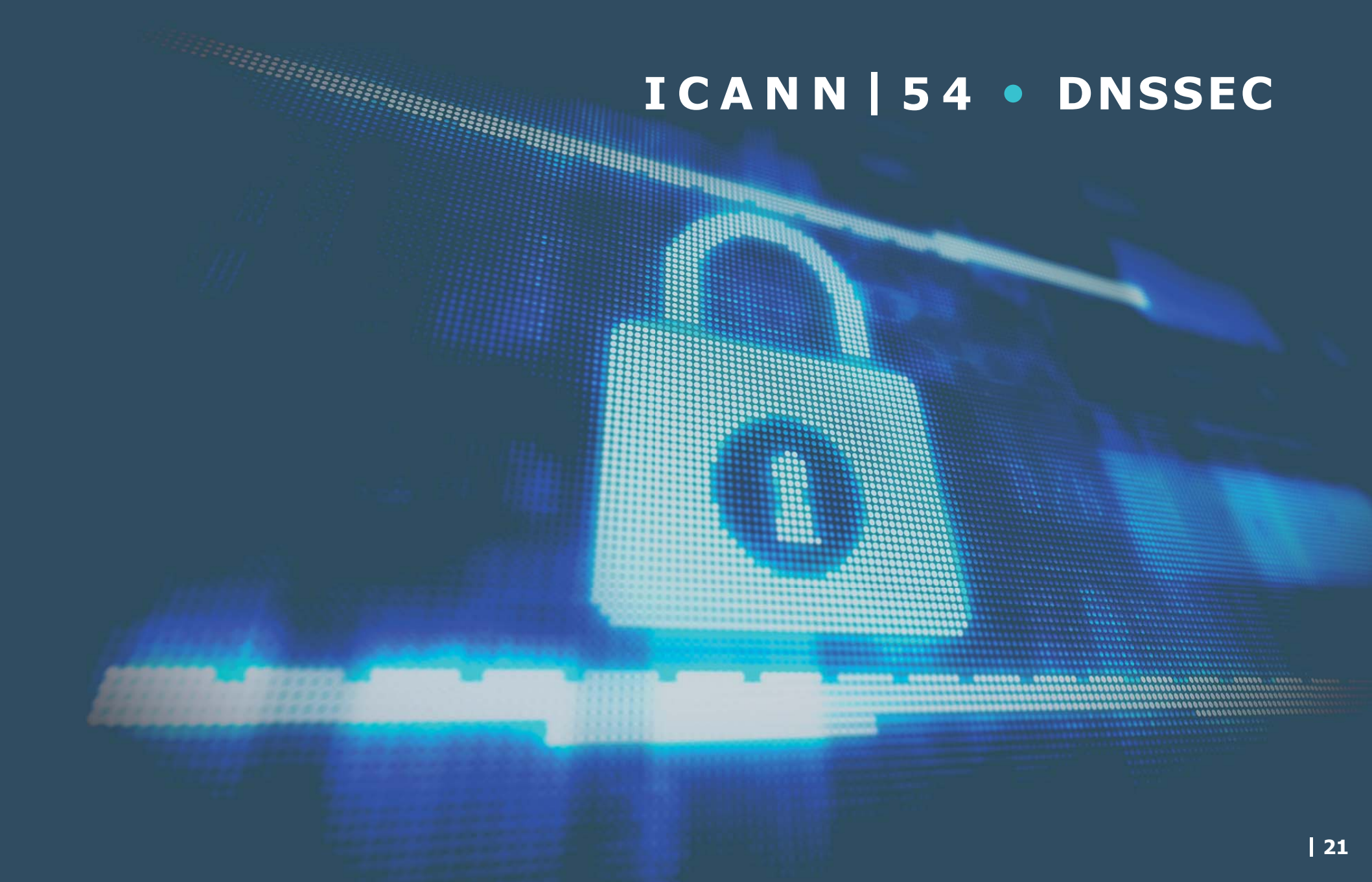
The Turris Project:
Filip

Ondřej Filip do .CZ o ccTLD da República Checa, fez uma atualização do projeto Turris. Trata-se de um projeto iniciado em 2013, com o objetivo de aumentar a segurança do utilizador final. No âmbito deste projeto foram fabricados e distribuídos pelo .CZ equipamentos de routing semelhante ao que os operadores instalam no serviço Internet residencial, tal como sucede em Portugal.

Os equipamentos foram distribuídos apenas na República Checa a um custo simbólico de 1 coroa checa, cerca de 0,04 €. Tratam-se de equipamentos com bastantes funcionalidades nomeadamente relacionadas com segurança.

Estes equipamentos já permitiram detetar algumas situações peculiares, nomeadamente o caso de uma smartTV que estava a fazer comunicações fora do normal para um local remoto.

O projecto está numa fase de expansão a novos paradigmas, nomeadamente o recente Internet of Things (IoT). A nova geração do equipamento terá um novo nome e uma nova marca, Turris Omnia, o .CZ pretende lançar uma campanha de crowdfounding para reunir recursos e ter uma perceção do interesse da comunidade em geral, o fabrico da nova geração está previsto para o primeiro quadrimestre de 2016.




Enter

Workshop DNSSEC

A sessão de trabalho dedicada a DNSSEC, conhecida por "Workshop DNSSEC" ocorreu no passado dia 21 de outubro, como já é habitual esta sessão faz parte da calendarização em todas as reuniões do ICANN.

Também como é habitual, os trabalhos começaram com um ponto de situação de DNSSEC, apresentado por Dan York da Internet Society. Recorrendo as medições de Geoff Huston da APNIC, verifica-se que atualmente, em termos globais, apenas 14% das consultas DNS com DNSSEC são validadas nos *resolvers* DNS, muito frequentemente no serviço de DNS Público da Google. Apesar de ser um número modesto, este valor continua a crescer de forma geral. Em termos regionais, e no caso concreto no espaço Europeu verifica-se que já existem países com uma alta taxa de validação DNSSEC, 5 deles acima de 50%, e onde a utilização do serviço DNS da Google é baixa, o que significa que está a ser feito um trabalho pelos ISPs e operadores de rede nesse sentido, ou seja estão a adotar DNSSEC. Esta é considerada a ultima milha, para o objetivo a que o DNSSEC se propõe, tornar o serviço DNS mais seguro.

Dan York também apresentou as medições de Rick Lamb do ICANN disponíveis online em "https://rick.eng.br/dnssecstat/". Dos 1.080 domínios de topo (TLD) existentes à data de medição a 20 de outubro, 909 estão assinados com DNSSEC, o que representa uma taxa de adoção de DNSSEC de 84% sendo que este número é global, ou seja inclui todos os ccTLD's, gTLD's e restantes TLD's. É um portanto um valor influenciado pelos recentes domínios de topo, onde DNSSEC é um dos requisitos mandatórios desde do início do processo de criação.

Destas medições também se constata que a nível de ccTLD's, a zona geográfica com mais trabalho por fazer é sobretudo o continente Africano, ainda, alguns países da Asia/Pacífico e da América central.

Em termos comparativos nos TLD's com DNSSEC, em outubro o .PT situou-se nos 11.955 domínios assinados com DNSSEC, fora do top 5 em termos absolutos, onde constam os seguintes TLDs ordenados pelo número de domínios com DNSSEC. É de realçar porém, que a grande maioria de ccTLDs com DNSSEC tem um número de domínios assinado com DNSSEC inferior ao .PT.

Classificação	TLD	Data da assinatura	% domínios c/DNSSEC	Domínios com DNSSEC / Total domínios
1º	.NL	2010/11/11	43.95%	2464494/5607305
2º	.BR	2010/06/23	22.25%	830546/3733607
3º	.SE	2010/08/27	46.46%	586298/1262057
4º	.COM	2011/03/31	0.45%	533712/119659915
5º	.CZ	2010/06/24	61.61%	464766/754333

Esta sessão foi importante para o DNS.PT, porque além de assistir aos trabalhos, a partilha de conhecimentos, o networking e as demais mais valias de uma presença no evento, tivemos oportunidade participámos no painel de oradores, Sara Monteiro apresentou à audiência as respostas colocadas previamente pelo comissão organizadora da sessão, e deu um ponto de situação de DNSSEC no .PT, no âmbito do painel "DNSSEC Activities in the European Region".

Ainda dentro do painel das atividades DNSSEC na Europa, foram feitas as seguintes apresentações:

Ondrej Filip, do .CZ, República Checa
DNSSEC .CZ

Cristian Hesselman, .NL, Holanda
SIDN DNSSEC Workshop Panel

Peter Janssen, .EU, Europa
DNSSEC in .EU

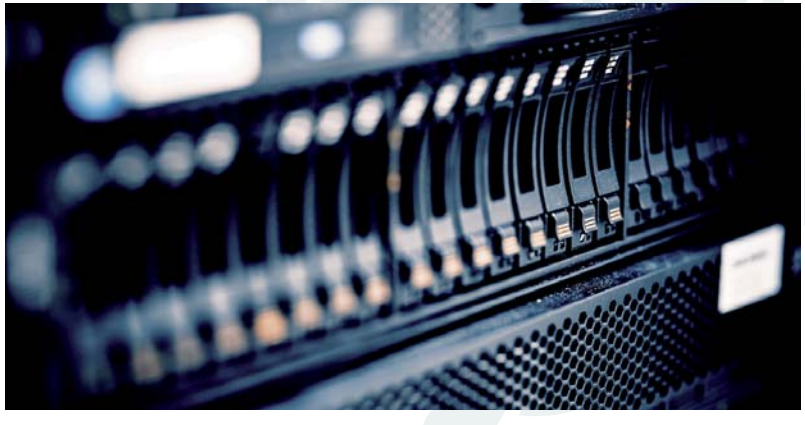
Peter Koch, .DE, Alemanha
DNSSEC Activities in .DE

Vincent Levigneron, .FR, França
DNSSEC Status (Operational View)

Roland van Rijswijk, Surfnet
Making the Case for Elliptic Curves in DNSSEC

Jacques Latour, do .CA, Canadá, foi moderador do painel de discussão "DNSSEC on the Edge", ou seja formas e soluções que utilizam DNSSEC com metodologias diferentes das habituais, para fazer face a desafios exigentes.

Ólafur Guðmundsson, da CloudFlare, apresentou o tema "DNSSEC Signing at Scale on the Edge". A CloudFlare é uma empresa de *Content Delivery Network* (CDN) em larga escala, com uma taxa de expansão muito elevada, e está a trabalhar para adotar DNSSEC na sua infraestrutura. No entanto a dimensão é neste caso, um fator decisivo, que implica pensar em DNSSEC de uma forma como ninguém o fez até ao momento. Nomeadamente, destacam-se a utilização de uma única chave Key Signing Key (KSK) para todos os clientes, o processo de assinatura que ocorre nos extremos da infraestrutura, a utilização de algoritmos de encriptação da família *Elliptic curve cryptography* (ECC), e por ultimo uma abordagem minimalista nas respostas DNS negativas.



Jacques Latour, do .CA, Canadá apresentou o tema "DNS Operator Role Bootstrapping DNSSEC Chain of Trust". O problema identificado pelo .CA, é a entrega do registo de *Delegation Signer* (DS) de um operador DNS para o Registry, e a consequente gestão DNSSEC dos domínios. Por operador DNS entenda-se uma das seguintes entidades: o Registrar, o Titular do domínio, o serviço de alojamento, ou uma rede CDN, ou outra. Ou seja, como é que entidades que não entram no modelo standard (Registry/Registrar/Registrant) podem operar domínios com DNSSEC?

A solução proposta pelo .CA é uma interface de comunicação com operadores DNS, para que estes possam gerir domínios com DNSSEC sem quebrar a cadeia de confiança fornecida pelo DNSSEC. Numa fase inicial o registo DS é gerado e enviado para o Registry. Numa fase posterior o *Registry* fica responsável pela gestão DNSSEC desses domínios. Desta forma o Registry garante que o processo DNSSEC executa corretamente, em nome do bom funcionamento da Internet.

Dan York, da Internet Society, foi o moderador do secção de "DANE and Applications". DNS-based Authentication of Named Entities (DANE) é apontado por muitos como a primeira aplicação massiva que irá tirar partido da segurança no DNS disponibilizada pelo DNSSEC. Este protocolo permite a associação de certificados X.509, vulgarmente utilizados para encriptação das comunicações, ou seja Transport Layer Security (TLS), em domínios DNS. Em suma, a utilização desta tecnologia pode vir a dispensar no futuro as atuais entidades de certificação, como a Verisign, a Multicert entre outras.

Dentro desta seção foram feitas as seguintes apresentações/demonstrações:

Sara Dickinson, Sinodun
DNSSEC for Legacy Applications

Wes Hardaker, Parsons
DANE Secured E-mail Demonstration

JRichard Lamb, ICANN
Outlook and SMIME/DNSSEC: Missing Link Found

Paul Wouters, Red Hat
DNSSEC/DANE Demo

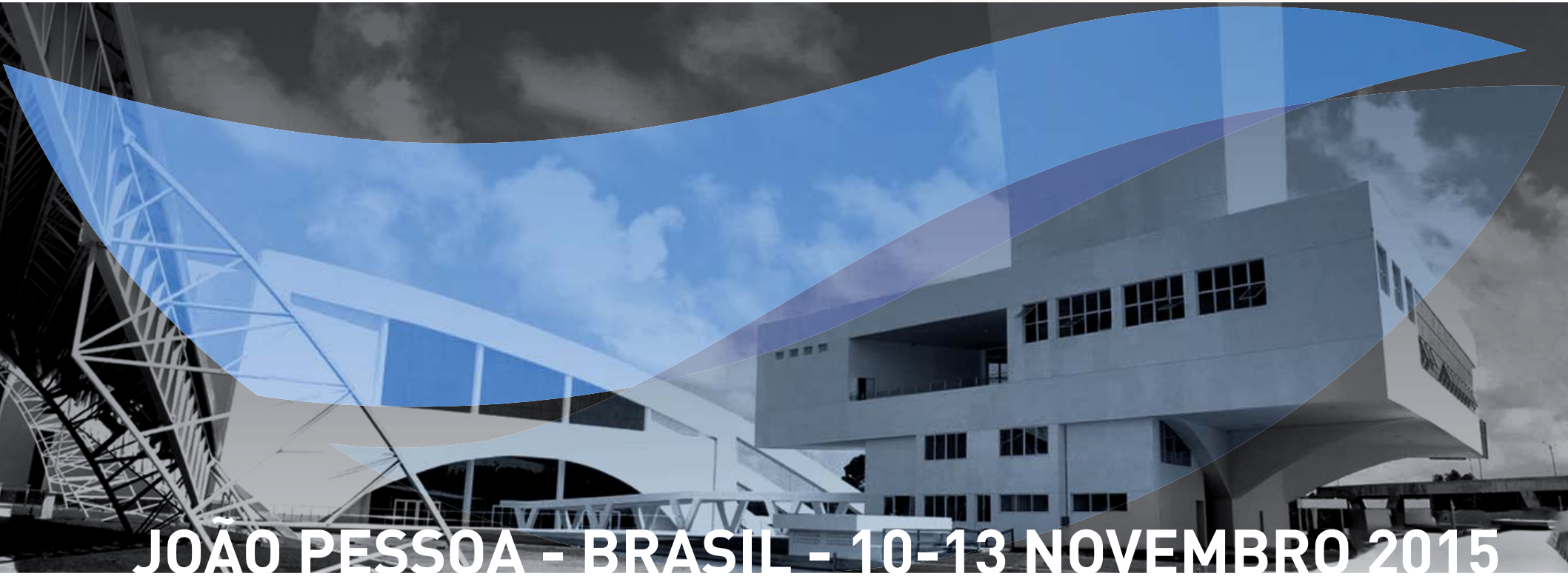
Em suma, o Workshop DNSSEC realizado no ICANN 54 em Dublin, foi uma boa demonstração do estado de maturação do protocolo DNSSEC. Acima de tudo permitiu constatar uma tendência crescente de considerar DNSSEC o standard, e o surgimento de aplicações que tiram partido desse standard como o Dane. Ou seja, a partir de agora irá surgir um novo conjunto de aplicações que têm por base o serviço DNS, com mecanismos de segurança.

dns.pt
dnssec.pt
facebook.com/dns.pt
pt.linkedin.com/in/dnspt

Produção: dezembro 2015
Grafismo: dns.pt

INTERNET GOVERNANCE FORUM 2015

IGF 2015
João Pessoa, Brasil



JOÃO PESSOA - BRASIL - 10-13 NOVEMBRO 2015

EVOLUÇÃO DA GOVERNANÇA DA INTERNET: CAPACITAR O DESENVOLVIMENTO SUSTENTÁVEL

O IGF[1] decorreu entre os dias 10 e 13 novembro de 2015, em João Pessoa, Brasil, sob o tema "A evolução da governação da Internet: Capacitar o Desenvolvimento Sustentável". O evento foi organizado pelo Comitê Gestor da Internet, onde está integrado o NIC.BR, sob os auspícios das Nações Unidas e contou com a participação de 2.400 pessoas oriundas de 116 países.

Como é sabido o Brasil tem liderado em muito a discussão da governação da Internet, a publicação do projeto de lei 21626/11, de 25 de março de 2014, conhecido como o Marco Civil da Internet, documento precursor e assumido como a "constituição" que vai reger o uso da rede no Brasil definindo direitos e deveres dos utilizadores e prestadores de serviços, e que agrega princípios como a neutralidade de rede, a liberdade de expressão e a privacidade dos utilizadores e, um mês mais tarde, a organização da Net Mundial[2], vieram abrir portas para esta edição do IGF. Por outro lado, quando a questão da proteção dos direitos de autor na Internet tem cada vez mais lugar nestes fóruns de discussão, há que reconhecer a este país, com uma notável e reconhecida vocação criativa e onde o audiovisual emprega tantas pessoas como o turismo, uma voz de peso. Nestes dias, ouvimos muitas vozes de desalento reclamando uma ação efetiva na luta contra a pirataria e a violação dos direitos de autor na Internet Fugindo a posições extremistas foi reclamado um balanceamento entre a liberdade de expressão e a proteção dos direitos de quem cria e, por isso, gera valor.

[1] http://www.igf2015.br/
[2] https://www.netmundial.org/pt-br/princ%C3%ADpios; http://netmundial.br/

Nas mais de 100 sessões que decorreram ao longo dos quatro dias de trabalhos, para além das matérias relativas à governação da Internet, neutralidade da rede, cibersegurança, IPv6, direitos humanos na Internet, zero-rating, entre outros, um dos tópicos em destaque foi de novo a matéria dos conteúdos, que já tivemos oportunidade de referir como tendo sido também um dos tópicos em discussão na ICANN de Dublin. Outro tema transversal foi o da definição das medidas e iniciativas tendentes a conectar o próximo bilião de pessoas que hoje ainda não está ligado à Internet[3].

Vint Cerf[4], conhecido como sendo um dos pais da Internet e que, inclusivamente, esteve em Lisboa aquando da ICANN 2007, defendeu publicamente a necessidade da comunidade estar hoje profundamente atenta às questões da segurança. Acérrimo defensor de uma Internet una, não fragmentada ou balcanizada, defendeu serem fundamentais ferramentas como a encriptação e o DNSSEC[5] para combater os ataques ao Domain Name System, sendo pois determinante melhorar a sua segurança. Segundo Vint Cerf, estamos num momento onde os dados são agnósticos relativamente à localização, a definição desta última já não significa segurança. Uma forma de melhorar a segurança é a de encontrar um meio que ajude a determinar se o endereço de IP associado a um nome de domínio foi modificado por um terceiro não autorizado. Estamos aqui no chamado layer técnico, onde a defesa da adoção de mecanismos de encriptação chegou perto do nível de direito inerente a qualquer cidadão. Diga-se porém que, paralelamente, se destacou ainda a importância da sensibilização da comunidade, na aceção de consumidores e utilizadores em geral, para estas matérias, assim como para a importância da criação de mecanismos de auto-regulação (também chamada de soft law) em áreas sobretudo dirigidas às faixas etárias mais jovens.

'***Your laptop should be encrypted, your disk drive should be encrypted, your mobile should be encrypted***', Vint Cerf

[3] Segundo o Estudo da Economia Digital ACEPI/DNS.PT, o número de utilizadores da Internet em Portugal cresceu cerca de 36% nos últimos 5 anos. Atualmente, mais de 2/3 da população é utilizadora da Internet.

[4] Vice President and Chief Internet Evangelist da Google

[5] https://www.dns.pt/pt/dnssec/ambito/

As questões associadas à neutralidade da rede mereceram discussão acesa ao longo das várias sessões repartidas pelos quatro dias de trabalho. Em termos gerais, uma definição possível do princípio da neutralidade da rede dita que todo o tráfego Internet deve ser tratado sem discriminação, restrição ou interferência e independentemente do género, origem, destinatário ou tipo de conteúdo. Neste pressuposto, os players no processo, em concreto, os ISP's, devem pautar a sua atuação de acordo com este mesmo princípio, preservando a segurança e integridade da Rede, mitigando eventuais efeitos resultantes de, por exemplo, picos e congestão de tráfego e garantindo serviços de emergência no caso de força maior. Por outro lado cabe ainda neste âmbito aos ISP's disponibilizar informação concreta e transparente sobre a tipologia e nível de serviço prestado por forma a não gerar dúvidas no consumidor final.

Ora estamos aqui a ver a questão da neutralidade da rede de um ponto de vista quase estritamente económico[6], muito direcionado à cadeia, prestador (ISP)/consumidor, e neste fórum foi consensual a ideia de termos de ir para além desta perspetiva. Como dito, a cadeia tem outros elos, como sejam os governos, os fornecedores de conteúdos, os gestores de motores de busca e, no topo, todos os utilizadores da Internet. É neste contexto que a neutralidade da Internet deve ser analisada, olhando então para as matérias da privacidade, proteção de dados, concorrência, igualdade de oportunidades, liberdade de expressão, direitos humanos na Internet, etc.

[6] Um aparte apenas, a título de nota, para dizer que durante o IGF foram várias a intervenções que informaram haver já estudos credíveis onde muitos consumidores afirmavam claramente estar dispostos a pagar mais por determinados conteúdos em detrimento de outros.

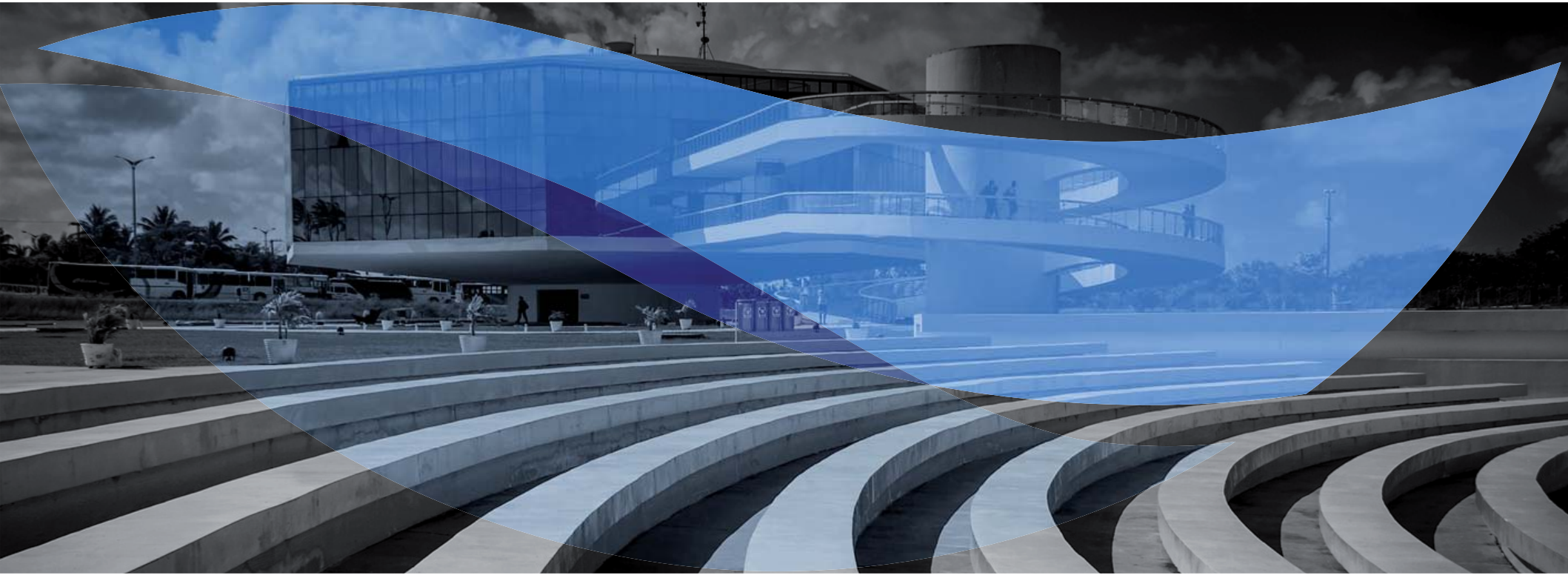
A este propósito uma das questões mais debatidas foi a do "zero-rating", esta matéria tem especial acuidade sobretudo para os países em desenvolvimento, em especial, os países Africanos, tendo assistido mesmo a várias intervenções em que era claramente afirmado que seria melhor o zero-rating que simplesmente nada... Vejamos, o zero-rating (taxa zero) é um "mecanismo" criado pelos ISP's em que simplesmente não é faturado qualquer valor ao utilizador para o acesso a determinadas aplicações/sites, por exemplo Facebook e Wikipedia. Por exemplo no Quénia e na Índia, a Airtel fez uma parceria com o Facebook para oferecer acesso gratuito a determinados websites. Alguns países pesaram já os prós e contras desta solução tendo-a expressamente vedado, é o caso por exemplo do Japão, do Chile, da Noruega, da Finlândia, da Lituânia, entre outros.

Resta saber se o "zero-rating" é bom ou mau, já que quem define à partida quais os websites a que o acesso é gratuito é o ISP conduzindo logo a vontade do consumidor, num comportamento por muitos apelidado de monopolista e anti concorrencial. Um dos argumentos sufragados foi o de que devemos olhar para a definição de Internet enquanto sistema global de redes de computadores interligadas e de onde brotam milhares de websites. Este mecanismo subverte este princípio sobre o qual nasceu a Internet. Mesmo em matéria de direitos humanos fundamentais o zero-rating, promovendo a sonegação do acesso generalizado à informação, pode contribuir para o não desenvolvimento ou, como disseram alguns, a manutenção nas "trevas" de alguns países. Será este o caminho para ligar o próximo bilhão?

Entretanto prevê-se que o mandato do IGF se estenda por mais 10 anos. Aguarda-se pois os últimos desenvolvimentos a decorrer em dezembro no âmbito do WSIS (World Summit on the Information Society)+10.

O IGF João Pessoa terminou com a repetida mensagem dos 3 S's: Safe, Secure and Stable Internet

dns.pt
dnssec.pt
facebook.com/dns.pt
pt.linkedin.com/in/dnspt



Produção: dezembro 2015
Grafismo: dns.pt

Marta Moreira Dias ● Assis Guerreiro

Produção: dezembro 2015
Grafismo: dns.pt