ICANN 58
COMMUNITY FORUM

COPENHAGEN
11-16 March 2017

RELATÓRIO DNS.PT

ÍNDICE

Sumário executivo

Na ICANN58[1], reuniram-se mais uma vez, o setor privado, os governos, a comunidade técnica e a sociedade civil para discutir uma variedade de tópicos de revelo para os TLD´s[2]. Após uma análise sobre aquilo que se perspectiva ser o caminho para a sustentabilidade dos ccTLD´s, iremos debruçar-nos, em especial, sobre a questão dos dois caracteres como domínios de segundo nível e dos nomes de países e territórios nos novos gTLD´s[3], e GDPR[4].

Introdução

A edição 58 da ICANN decorreu, entre os dias 11 e 16 de março, em Copenhaga, na Dinamarca. O Anfitrião desta ICANN foi a DIFO[5], associação responsável pela gestão do ccTLD .dk, fundada em julho de 1999 , e que se apresenta com um slogan emblemático: " We administer the Danish part of the internet".

Na abertura da ICANN58, marcada pelos discursos da Ministra da Cultura da Dinamarca, Mette Bock e pelo Presidente da DIFO, o Professor HenriK Udsen, foi mencionada a necessidade de aumento de esforços para o combate à cibercriminalidade, a atenção generalizada que se impõe face aos desafios do GDPR, e a necessidade de gerar valor Core aos nomes de domínio. Ambos os discursos teceram notas elogiosas ao modelo multistakeholder hoje adotado em grande parte dos ccTLDs mundiais, condição sine qua non para o respetivo crescimento e sustentabilidade.

1 *A ICANN (acrônimo em inglês para Corporação da Internet para Atribuição de Nomes e Números) é uma organização sem fins lucrativos de benefício público com participantes de todo o mundo, que se dedica a manter a Internet segura e estável, promovendo a concorrência, sendo responsável pela alocação do espaço de endereços do Protocolo da Internet (IPv4 e IPv6), pela atribuição de identificadores de protocolo, pela administração do sistema de nomes de domínio de primeiro nível genéricos (gTLDs) e pelos códigos de países (ccTLDs), assim como pelos sistemas de servidores-raiz.*

2 *Top-Level Domain).*

3 *Domínios de topo genéricos (generic top-level domains).*

4 *General Data Protection Regulation*

5 *A DIFO é uma associação sem fins lucrativos cujos membros representam a comunidade dinamarquesa da Internet, incluindo fornecedores (IBFO, a Associação Dinamarquesa de Indústrias de TI), utilizadores profissionais (a Confederação da Indústria Dinamarquesa, a Câmara de Comércio Dinamarquesa) e utilizadores privados (o Conselho do Consumidor e a Sociedade Dinamarquesa de TI).*

Nesta edição o DNS.PT alargou a sua equipa de participantes, tendo incluído dois dos seus colaboradores mais jovens, uma jurista e um especialista em segurança informática, que tiveram oportunidade de vivenciar a dinâmica de uma reunião da ICANN. O presente relatório traduz, em praticamente toda a sua plenitude, a visão destes dois colaboradores destes cinco dias de trabalhos.

"*Como newcomer, tive oportunidade de ter voz ativa, como parte de uma comunidade que preza pela liberdade de expressão, sentindo que pude envolver-me na definição futura da política da internet". Mais do que conhecimento, presenciei uma experiência de verdadeiro contato com um modelo democrático de governação da internet, do século XXI", cujo grande objetivo de manutenção da confiabilidade e estabilidade da internet, a todos diz respeito. Acredito que o modelo criado para a governação da internet, que inclui, o setor privado, os governos, a sociedade civil e a comunidade técnica, é fundamental para se estabelecerem princípios, normas e regras que moldam o nosso futuro e onde cada um tem o seu papel, garantindo a transparência no DNS mundial. As discussões sobre as políticas estão abertas a todos os interessados, as sessões de discussão são transmitidas na internet e a documentação é livremente acessível à comunidade. A todos é concedido o mesmo estatuto em pé de igualdade*".

Luisa Cyrne, Jurista no DNS.PT.

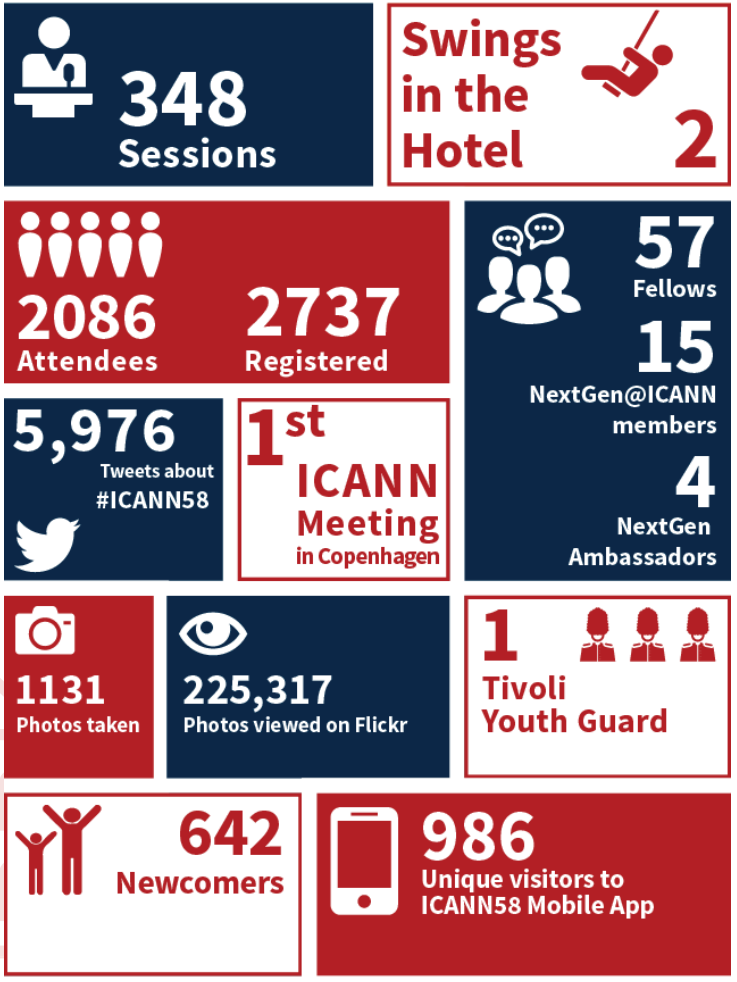
"*No meu primeiro ICANN, tive oportunidade de presenciar como este órgão atua nos seus diferentes grupos de trabalho, onde todas as partes interessadas têm oportunidade de participar e contribuir para o futuro da internet, mantendo a segurança e a confiança deste espaço. Destaco o incrível ambiente de cooperação e partilha entre os participantes.*"

Ricardo Pires, Técnico de Segurança
da Informação no DNS.PT.

A ICANN 58 foi impactante não só pela importância dos temas discutidos, como ainda pela recente transição da supervisão das funções da IANA, em 30 de setembro de 2016, que até então estavam sob o controle do Departamento do Comércio dos Estados Unidos da América, para a responsabilidade da PTI[6]. Ora, como o processo de transição é muito recente, gerou-se um grande foco nas discussões sobre a continuidade dos trabalhos em torno do tema da accountability da ICANN[7]. Na ausência da supervisão dos EUA nos moldes anteriormente vigentes, a comunidade tem agora novas ferramentas para responsabilizar e, quando necessário, sancionar a organização.

Destaca-se também o encontro da LusNIC- Associação privada de Registries de Língua Portuguesa, no dia 12 de março, para a concretização da segunda assembleia geral, que culminou com a aprovação do Plano de Atividades para os anos de 2017/2018[8].

ICANN 58 em números



6 *Public Technical Identifiers - Empresa entidade subsidiária da ICANN que será responsável por conduzir e operar as funções IANA.*

7 *Reunião presencial do CCWG Accountability.*

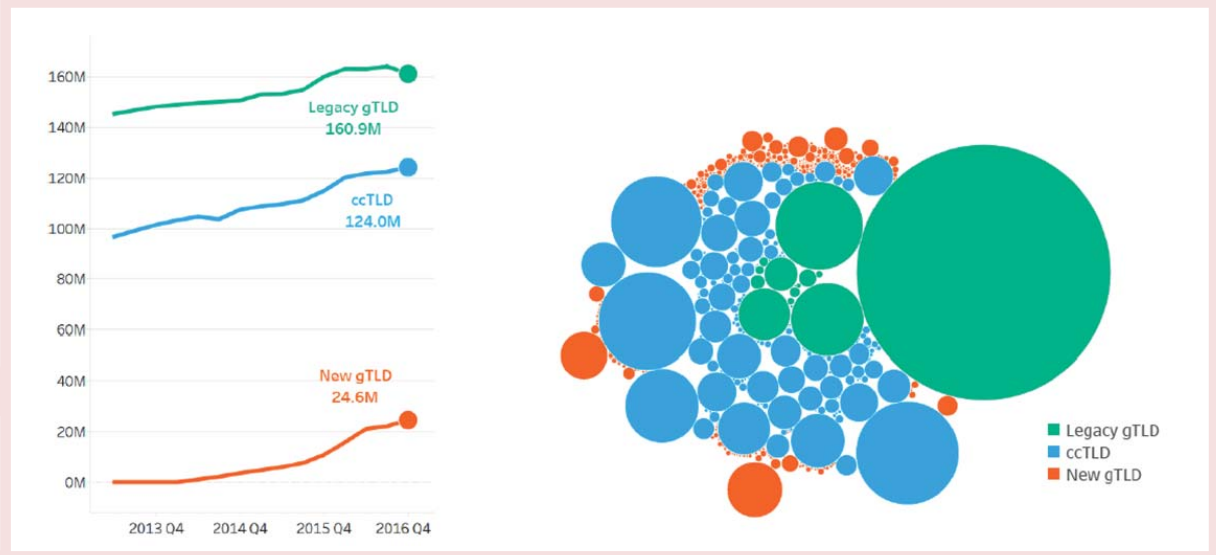
8 *A LusNIC junta as entidades competentes pela gestão, registo e manutenção de domínios de topo (ccTLD's, country code Top Level Domains) dos países de língua oficial portuguesa. Estas entidades, também designadas de Registries, representam: .pt, de Portugal o .br, do Brasil, o .cv, de Cabo Verde, o .gw, da Guiné-Bissau, o .st. de São Tomé e Príncipe e o .ao de Angola e tem por objecto a cooperação institucional multilateral entre os Registries de língua portuguesa no âmbito das suas áreas de intervenção.*

ccTLD's em perspetiva: sustentabilidade

Uma das questões que tem sido recorrente em fóruns como a ICANN, mas também no CENTR, é a da avaliação sobre a sustentabilidade dos ccTLD's, sobretudo após a entrada no mercado dos mais de 1200 novos gTLD's. Hoje, longe que estamos da estrita e redutora dualidade ccTLD's/legacy gTLD's, a tendência será mesmo falar de um novo mercado global ao nível do registo de domínios. Mas o problema – se há problema - não fica por aqui. A utilização crescente das APP's, blogs e das redes sociais apresenta-se com números arrebatadores e difíceis de acompanhar, senão veja-se, olhando apenas para a fotografia deixada pelo Facebook: 1.7 biliões de contas ativas "contra" pouco mais de 300 milhões de nomes de domínios.

Se pensarmos que estes 300 milhões estão ainda repartidos entre os legacy gTLG, os ccTLD's e os new gTLD, então permitimo-nos afirmar que o cenário fica ainda mais complicado.

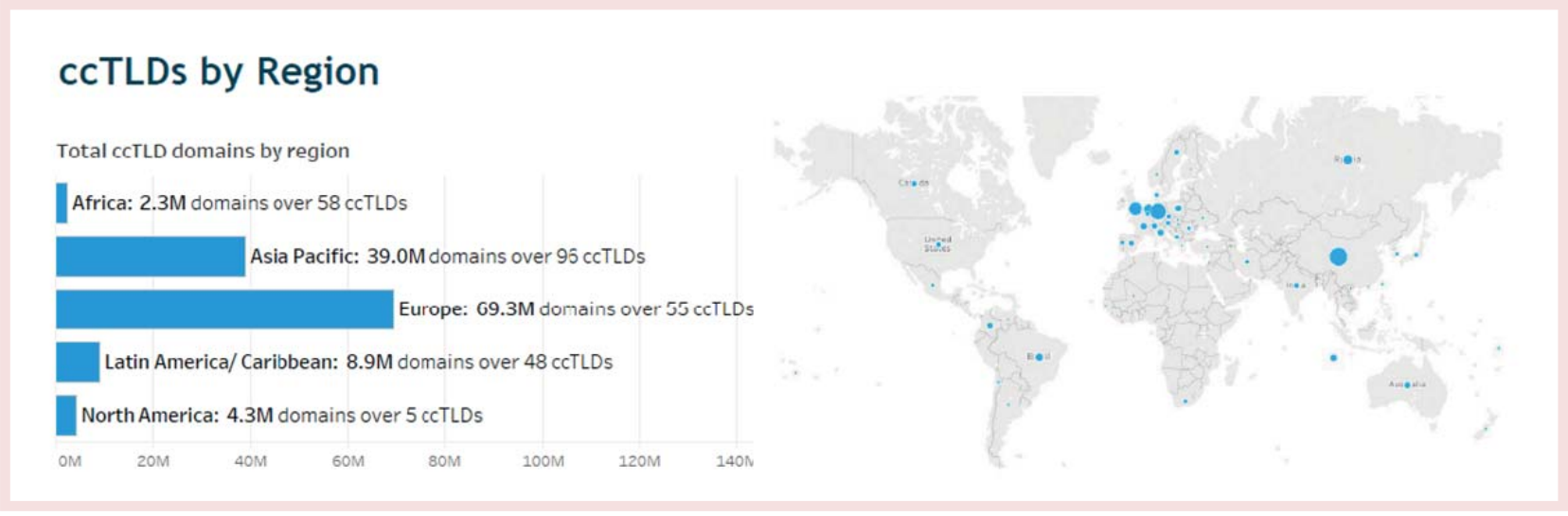
Divisão do mercado entre os gTLD's



Fonte: CENTR

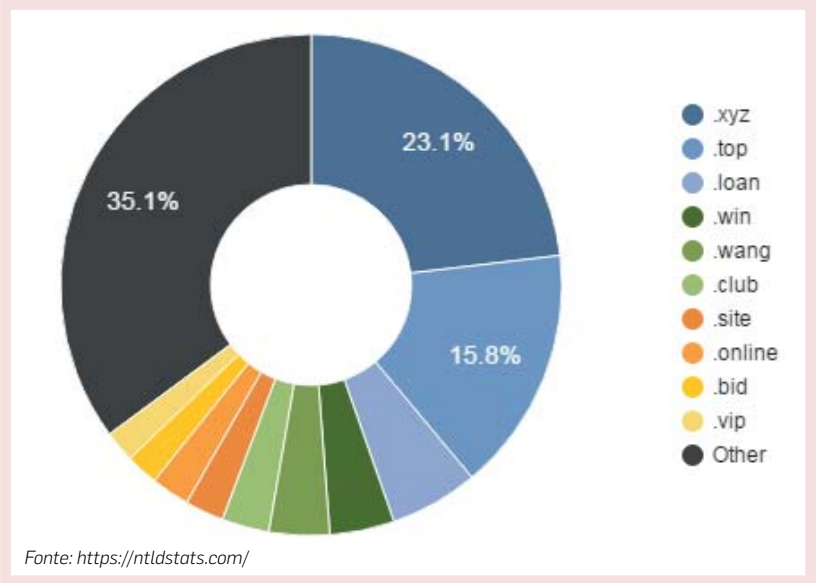
Se fizermos uma análise mais fina, facilmente percebemos que a quota de mercado dos ccTLD's face aos gTLD's não é equilibrada e TLD's como o .com continuam a liderar o mercado, embora com um notado decréscimo registado logo a partir de 2015.

ccTLD's por região



Fonte: CENTR

Distribuição de registos entre os principais gTLD's

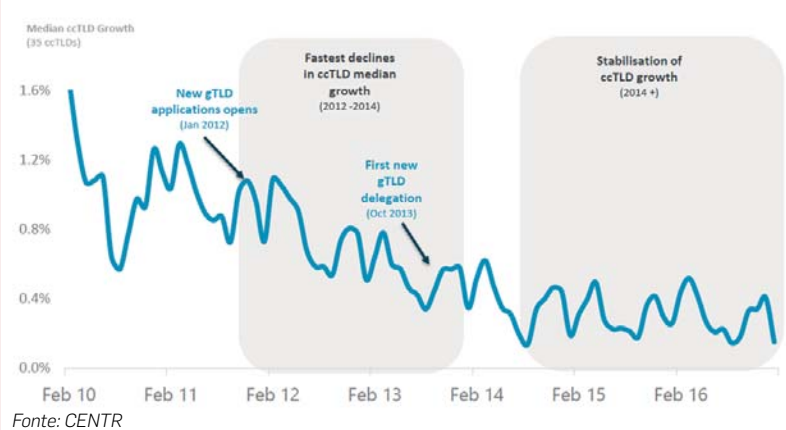


Fonte: https://ntldstats.com/

O cenário europeu perspetiva-se neste momento como estável, existem cerca de 70 milhões de domínios registados, com países como a Arménia, .am, Estónia .ee e Portugal .pt a liderar o ranking dos ccTLD's que mais cresceram. Em .pt foram registados em 2016 94 507 domínios, verificando-se uma confortável taxa de retenção de, aproximadamente, 80%.

Ou seja, hoje os ccTLD's europeus apresentam uma taxa média de crescimento de 3.4%, o que, comparativamente com os anos que se seguiram ao processo de abertura das candidaturas aos novos gTLD's e das primeiras delegações, é manifestamente positivo e demonstra que o mercado está a estabilizar. De taxas de crescimento superiores a 12% que se registavam em meados de 2011, passou-se rapidamente para percentagens de 5.6 em 2013. Só a partir do final de 2014 estes números tenderam a estabilizar num valor próximo aos 3.4% já enunciados.

Evolução do registo face à entrada no mercado dos novos gTLD's



Fonte: CENTR

Resta encontrar o que esteve na base desta estabilização do mercado que ainda há poucos anos se afigurava como muito temida pelos ccTLD's. Cumpre, no entanto, fazer aqui um pequeno parênteses para reiterar o facto desta estabilização não significar ainda sustentabilidade[9]. Desde logo, não pode ser desconsiderado o facto dos novos gTLD's[10] poderem vir a aumentar a sua quota de mercado,

9 *Curiosamente correm já na Internet pequenos surveys sobre onde estará o mercado de domínios daqui a 10 anos. Veja-se: https://www.thedomains.com/2017/03/22/believe-domaining-will-still-viable-business-2027/*

10 *O .eu, não sendo um gTLD não deve ser esquecido quando falamos de concorrência, sobretudo para os ccTLD's. Em Portugal, no ano de 2016, estavam registados 16 564 domínios sob .eu.*

o que certamente terá impacto no registo sob os ccTLD's pois claramente divide o mercado. Depois a conjuntura económica de cada país e a consequente evolução do tecido empresarial são variantes a considerar nesta equação, pelo que o futuro é ainda incerto. De qualquer forma, os números são objetivos, mantendo-se o crescimento nos níveis médios identificados acima. Ou seja, argumentos como a diminuição do número de remoções e de não renovações e o facto dos legacy gTLD's terem baixado ligeiramente a sua taxa de penetração para os 35 pontos percentuais, concorrem para justificar a dita estabilização. Em Portugal, como em muitos congéneres da Europa e sobretudo ao nível dos registries de menor dimensão, tem havido igualmente uma grande aposta na divulgação, o que tem contribuído para pôr a marca .pt naquilo que em gíria se chama o radar do mercado, e isto com frutos visíveis se olharmos para a nossa evolução de registo[11].

Conclui-se pois que neste momento o mercado é incerto e as variantes são pouco previsíveis, cabe pois aos ccTLD's encontrar opções que lhes garantam a respetiva sustentabilidade. As alternativas agora apresentadas nesta última edição da ICANN passam por eventuais ajustamentos ao preço final dos domínios, diminuição de custos de funcionamento, procura de novos segmentos de mercado e, muito relevante e unanimemente aplaudido pelos representantes dos ccTLD's presentes, a chamada diversificação da atividade. Neste campo cabem atividades como a recentemente lançada pelo .pt, o Selo CONFIO[12]. Neste último caso o ccTLD entra num segmento de mercado que não sendo o registo de domínios, está fortemente relacionado com a confiança, legalidade e segurança da utilização da Internet, ou seja, mantém com isso uma linha orientadora que vai ao encontro da sua missão definida estatutariamente[13].

11 *Estatísticas de registo: https://www.dns.pt/pt/estatisticas/?tipo=0&ordem=0&ano=2016&graph=0&subm=Filtrar*

12 *Parceira DNS.PT, ACEPI e DECO - selo de acreditação de sites. Informação adicional: www.confio.pt*

13 *Estatutos disponíveis para consulta em: https://www.dns.pt/fotos/editor2/estatutosdns_2016v2.pdf*

Códigos de dois e três caracteres, nomes de países e territórios nos novos gtld´s

Concentremos agora a nossa atenção em dois grandes tópicos de discussão na ICANN58 e que têm especial acuidade para os registries em geral.

A questão dos códigos de países e nomes de países e territórios no âmbito do programa de novos gTLDs, continua a ser um tema controverso e que tem gerado alguma fricção entre o GAC[14]e a GNSO[15]. Em Copenhaga questionou-se a possível incoerência das decisões do Board a este respeito. Ora, recapitulando, em 1 de Dezembro de 2014 a ICANN[16] autorizou a liberalização dos códigos de países de dois caracteres especificados na ISO 3166/2, no segundo nível nos novos gTLDs, no sentido de promover a concorrência no mercado de nomes de domínio, desde que o governo e o Registry do país interessado fosse notificado para se pronunciar[17].

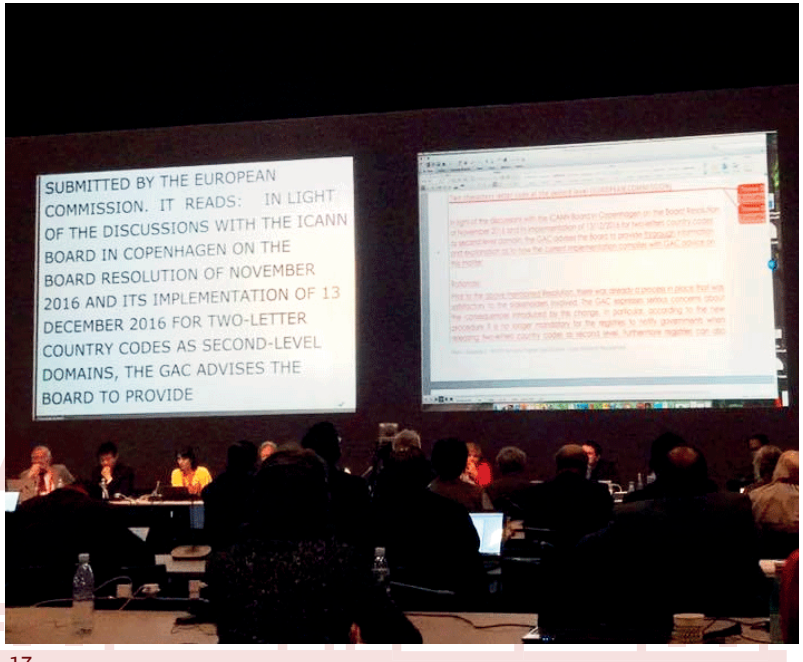
14 *Governmental Advisory Committee -A ICANN recebe a contribuição dos governos por meio do Comitê Consultivo Governamental (GAC). O papel fundamental do GAC é fornecer aconselhamento à ICANN sobre questões de políticas públicas e, especialmente, onde possa haver uma interação entre as atividades ou políticas da ICANN e as leis nacionais ou acordos internacionais. O GAC geralmente reúne-se três vezes por na ICANN, onde discute questões com o Board da ICANN e outras organizações de apoio da ICANN, comitês consultivos e outros grupos.*

15 *The Generic Names Supporting Organization - Organização responsável pelas políticas dos domínios genéricos de nível superior (por exemplo, .com, .org, .biz). A GNSO esforça-se para manter os gTLDs a operar de forma justa e ordenada numa Internet global, promovendo simultaneamente a inovação e a concorrência.*

16 *A primeira fase do procedimento foi a autorização para a liberação de etiquetas ASCII de dois caracteres. A finalização deste procedimento deu-se com a implementação de um quadro contendo medidas padronizadas em que os Registries podem implementar para evitar confusão, de acordo com o Acordo com os Registries e permitir a liberação de todos os rótulos ASCII de letras e letras de dois caracteres correspondentes aos códigos de país não Reservado de acordo com a Especificação 5, Secção 6 do Contrato de Registro.*
https://www.icann.org/en/system/files/files/spec5-amend-two-char-01dec14-en.pdf
Visto que a Especificação 5, Secção 2 do Acordo de Registo de novos gTLDs exige que os Regsitries reservem rótulos ASCII de dois caracteres dentro do TLD no segundo nível, os rótulos de dois caracteres reservados "podem ser liberalizados na medida em que o Registry chegue a acordo com o governo e o Registry que gere o código do país relacionados com a string, conforme especificado na norma ISO 3166-1 alpha-2. O Registry também pode propor a liberalização dessas reservas com base em sua implementação de medidas para evitar confusão com os códigos de país correspondentes, sujeito à aprovação da ICANN ".
https://www.icann.org/resources/board-material/resolutions-2016-11-08-en#2.a

desde que o governo e o Registry do país interessado fosse notificado para se pronunciar[17].

O gTLD Registry que pretendesse a utilização dos códigos com dois caracteres de países especificados na norma ISO 3166/2, tinha duas opções, ou interpelava diretamente o governo e a entidade gestora do ccTLD em questão, sobre a sua permissão para a utilização desses códigos ou solicitava essa aprovação diretamente através da ICANN. Na última opção, os governos seriam notificados, ou pelo menos os que o queriam o ser, e tinham 60 dias para oposição. Os interesses de ambas as partes estavam pois tutelados.



17 *O GAC, inclusive, criou uma lista pública 12 de países que dispensam notificações como forma de agilizar o processo.*

O panorama mudou com a resolução do Board tomada em 8 de Novembro de 2016, em Hyderabd, e a sua implementação, em 13 de dezembro de 2016[18], que permitiu a liberalização de todos os códigos de dois caracteres previamente reservados, facto que terá surpreendido a comunidade.

Nesse mesmo sentido algumas vozes discordantes fizeram-se ouvir no GAC e no ccNSO. Esta autorização geral, materializada no cancelamento do período de resposta de 60 dias, gerou discordância de alguns governos parte do GAC, que tinha dado parecer ao Board no sentido oposto. Embora haja dentro do próprio GAC, países e territórios que defendem a posição do Board, outros defendem que está em causa o interesse público, pelo que salvo se o governo ou o Registry que é responsável pela gestão do código do país tenha prestado o seu consentimento através de uma carta formal, tal não deverá ser permitido. Consequentemente, a ICANN58 foi marcada pela insatisfação do GAC nesta matéria. O GAC vai mais além, afirmando mesmo que não houve transparência na condução deste processo de liberalização e que a utilização dos códigos de dois caracteres pelos novos gTLD's devem permanecer reservados aos ccTLDs. Mais, na perspetiva do GAC o conjunto de requisitos impostos pela ICANN são muito pouco exigentes, não protegendo os ccTLDs.

18 *Após esta decisão o GAC aconselhou o Board da ICANN a:*
I. Tomar em consideração as graves preocupações expressas por alguns membros do GAC Contidas em conselhos dos GAC anteriores;
II. Envolver-se com os governos interessados na próxima reunião da ICANN para reocupações;
III. Tentar encontrar rapidamente medidas com o objetivo de encontrar uma solução satisfatória de acordo com as preocupações desses países;
IV. Proporcionar esclarecimentos sobre o processo de tomada de decisões e os fundamentos, nomeadamente sobre a resolução tomada em 8 de novembro de 2016, particularmente no que diz respeito ao aconselhamento, calendário e nível de apoio do GAC para esta resolução.

Um segundo problema intrínseco ao primeiro está relacionado com a utilização pelos novos gTLDs de códigos de três caracteres de países ou territórios, especificamente aqueles que figuram na lista ISO3166 Alfa-3 e, igualmente, nomes completos de países e territórios, mas, desta feita, no primeiro nível.

O grupo de trabalho[19] sobre o uso de nomes de países e territórios como TLDs (CWG-UCTN) responsável pelo tema, divulgou em 9 de fevereiro de 2017, um relatório que se encontra em consulta pública até o dia 21 de abril[20], com o objetivo de obter feedback e respostas da comunidade sobre o caminho a seguir.

O CWG-UCTN adiantou nas sessões públicas desta ICANN, a perceção que obteve dos seus membros e a dificuldade de criação de um quadro de referência consensual e harmonizado para a utilização de códigos e nomes de países no domínio superior[21]. Isto porque tanto as opiniões são distintas como existem processos paralelos em outros grupos de trabalho, como por exemplo, o grupo de trabalho do GAC sobre nomes geográficos. O projeto "GeoNames" do GAC centra o seu trabalho nos nomes geográficos que estão fora de qualquer lista ISO e tenta criar diretrizes para este assunto.

Do seu ponto de vista, há um vazio regulatório nesta matéria. Como tal, a solução encontrada pelo grupo de trabalho, seria a ICANN consultar toda comunidade para avaliar a possibilidade de criação de um catálogo de nomes geográficos para servir de guidelines aos novos gTLDs que ambicionam a utilização destes nomes. A finalidade desta solução seria a obrigatoriedade imposta aos novos gTLDs requerentes da utilização de nomes geográficos, de consulta a priori de uma lista. A ideia seria ainda, em caso de interesse num nome que conste da lista por um novo gTLD, que o governo em questão se pronuncie a favor dessa utilização. Ou seja, o processo de permissão de utilização de um nome geográfico a um gTLD, passaria por duas fases, em primeiro lugar pela verificação de uma tabela de nomes geográficos e, por fim, pela aprovação do governo do respetivo país ou território.

19 *Foi criado um grupo de trabalho intercomunitário patrocinado pela ccNSO e a GNSO com o intuito de estudar a viabilidade e o impacto que os códigos de 3 caracteres possam ter, no caso de se poderem registrar como gTLDs.*
Todos os documentos deste grupo de trabalho podem ser encontrados no wikispace do grupo.

20 *https://ccnso.icann.org/workinggroups/ccwg-ctn-interim- Paper-09feb17-pt.pdf.*

21 *Data de abertura do período de comentários do público: 21 de abril de 2017 , este trabalho será submetido aos conselhos da ccNSO e GNSO para discussão, adoção das próximas etapas.*
https://www.icann.org/news/announcement-2017-02-24-pt.

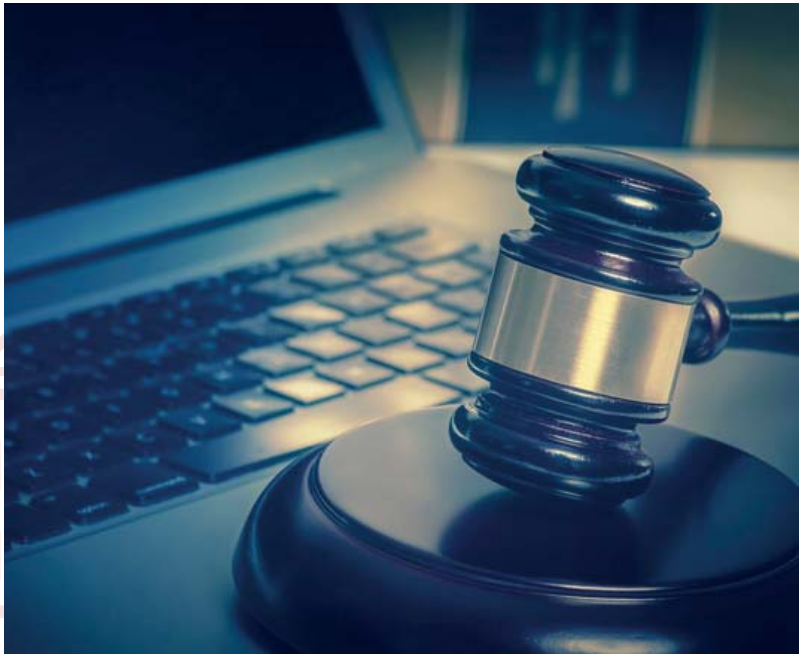
O CWG-UCTN, alinhado com esta posição concluiu dever-se sim, definir os nomes dos países e territórios, no entanto, não via ICANN, mas através, da organização internacional de normalização (ISO). Ambos os grupos de trabalho levantaram questões como a confusão que se gera para o consumidor, entre um código de um país de três caracteres e um gTLD, associado, por exemplo, a uma marca com uma conotação completamente distinta.
Outro ponto relacionado com este assunto, é o fato de existirem domínios já delegados que se confundem com códigos de países, como por exemplo, o .com, que apesar de ser um TLD genérico, figurar na lista ISO-3166 como o código específico para um país, neste caso Comores.

Em conclusão, esta matéria continua a ser motivo de discórdia em vários setores da comunidade, aguardamos os novos desenvolvimentos.

Como habitualmente, as questões de índole jurídico são amplamente discutidas neste fórum. Assunto recorrente é o de aferir as respostas dos ccTLD´s aos pedidos das autoridades nacionais para encerrar sites, especificamente para apagar um nome de domínio de suporte a um determinado site. Estes pedidos podem ter motivações diversas, ou por infrações ligadas à propriedade industrial, ou por motivos ligados a recolha de provas, ou por matérias de natureza penal, como crimes de pornografia infantil, tráfego de seres humanos, fraude, cibercriminalidade entre outros.

O problema reside sobretudo quando se colocam questões relativas à jurisdição. A título de exemplo, a questão de saber se determinada entidade de um país pode solicitar a remoção de um domínio com registo noutra jurisdição. O que significa que deverá existir um incremento ao nível da colaboração entre as partes envolvidas, assim como uma cooperação entre as autoridades competentes dos Estados Membros, a fim de se assegurar o cumprimento da lei.

Numa das sessões do ccNSO sobre esta temática, deu-se como exemplo, um Registry que no caso de lhe ser pedido a remoção de um nome de domínio, pelos motivos invocados no parágrafo anterior, por uma autoridade de outra jurisdição, só remove o mesmo por decisão do Tribunal competente desse país.



Em matéria de defesa do consumidor, a Proposta de Regulamento do Parlamento Europeu e do Conselho nº 2016/0148, de 25 de Maio de 2016, para defesa do consumidor, que tem por objeto, assegurar a segurança jurídica no Mercado Único, através da coerência na aplicação coerciva do acervo essencial da União em matéria de direito do consumo, é já um caminho nesse sentido.
A proposta de Regulamento estabelece as condições para que as autoridades competentes cooperem entre si e com a Comissão, a fim de assegurar o cumprimento da legislação em matéria de proteção do consumidor e o bom funcionamento do mercado interno. Para tal, são ativados mecanismos de alerta e de assistência mútua, complementados por um conjunto mínimo de poderes de que autoridades devem dispor, como "*Encerrar sítios web, domínios ou quaisquer outros sítios, serviços ou contas digitais similares*[22]", para uma cooperação transnacional eficiente e juridicamente sólida.

A este propósito, ouvimos também o testemunho do Registrar GoDaddy, que salientou que como Registrar, está contratualmente obrigado a, se solicitado, dar as informações que sejam pedidas tendo em vista a remoção do site. Nesse encargo, depara-se com o problema de jurisdição supra referido, nomeadamente, a questão de saber que autoridades têm competência para solicitar a remoção de um domínio. Assim, é preciso trabalhar neste aspeto, tanto os Registrars como os Registries, no caso de as autoridades solicitarem a suspensão ou remoção de nomes de domínio, carecem de saber com confiança, qual o fim daquele pedido, o objeto deste, qual é jurisdição nacional que está a ser violada e quanto tempo tencionam suspender o domínio, para que se torne claro o porquê da sua remoção. Como tal, foi dado e aplaudido o exemplo da Agência Nacional de Crime do Reino Unido, pela sua interação com a indústria de nomes de domínio, já que, por exemplo, verificam os pedidos antes de enviarem para hosters, Registries e Registrares e indicam desde logo qual é a entidade competente na matéria, a tipologia do crime em causa e a ação requerida pelas autoridades.

22 *Art. 8º, nº e, alínea l), da Proposta de Regulamento do Parlamento Europeu e do Conselho nº 2016/0148 de 25 de Maio de 2016.*

GDPR

Um dos temas de grande interesse voltou a ser a proteção de dados, tendo o grupo de trabalho RDP[23], o GAC e o ccNSO debatido o assunto em várias sessões repartidas ao longo desta última edição da ICANN. Discutiu-se em particular o novo quadro europeu de proteção de dados, decorrente do novo regulamento de proteção de dados[24], já vigente, e aplicável aos 28 Estados-Membros a partir do dia 25 de Maio de 2018 e que vem revogar a Diretiva 95/46/EC, do Parlamento Europeu e do Conselho de 24 de Outubro de 1995.

Quase em simultâneo com a aprovação do novo Regulamento Geral de Proteção de Dados, o Parlamento Europeu aprovou, a 6 de julho de 2016, a Diretiva 2016/1148, relativa a medidas destinadas a garantir um elevado nível comum de segurança das redes e da informação em toda a União. Em particular, consagra-se a obrigação de os Estados-Membros adotarem uma estratégia nacional de segurança das redes e dos sistemas de informação e estabelecem-se requisitos de segurança e de notificação para os operadores de serviços essenciais e para os prestadores de serviços digitais.

A utilização generalizada da Internet e a dinâmica acelerada da economia digital, em suma a revolução tecnológica ocorrida dos últimos anos fez pender sobre o legislador comunitário a obrigação de rever o quadro legislativo aplicável à privacidade em geral.

Foi especialmente referida a necessidade de se efetuar um balanço entre dois direitos, o direito à privacidade, direito fundamental consagrado em qualquer estado de direito democrático e o direito à livre circulação de dados pessoais. Para esse efeito referiu-se o exemplo da circulação de dados entre Registries e Registrars, fundamental para o funcionamento do negócio.

A grande preocupação da comunidade ICANN relativamente a esta temática é o tratamento de dados pessoais efetuado através do WHOIS[25], ferramenta utilizada por praticamente todos os Registries responsáveis por domínios de topo, inclusive pelo ccTLD.pt. Através do WHOIS é identificado o titular, o gestor, o responsável técnico e o enderenço IP de um domínio.

Neste sentido e com este novo paradigma, foram destacados alguns princípios do novo regulamento, nomeadamente (i) o princípio da limitação do tratamento, isto é, o facto de os dados só deverem ser recolhidos com vista à realização de tratamentos cuja finalidade esteja claramente determinada, (ii) o princípio da minimização dos dados, que estipula que só devem ser recolhidos os dados estritamente necessários à realização da finalidade do tratamento e (iii) o princípio da responsabilidade, que indica que o responsável pelo tratamento deve ser capaz de comprovar o cumprimento das obrigações decorrentes do novo regulamento.

23 *Registration Directory Services.*

24 *Regulamento (EU) 2016/679, de 27 de abril de 2016, relativo àproteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados), transposta em Portugal pela Lei de Proteção de Dados Pessoais, Lei n.º 67/98, de 26 de Outubro.*

25 *https://en.wikipedia.org/wiki/WHOIS*

Relevante é pois saber se o WHOIS como hoje o conhecemos atende às novas exigências previstas no GDPR ao nível da privacidade de dados. A este propósito colocam-se duas questões, em primeiro lugar, a de saber se todos os dados disponíveis no WHOIS são indispensáveis para o funcionamento da atividade, ou se por outro lado, existem dados que não o são. Assim sendo, os Registries devem olhar para o princípio da limitação do tratamento, para o princípio da minimização dos dados e para os dados pessoais divulgados no WHOIS e fazer essa avaliação. Outra questão inerente a esta, é o fato dos dados, no WHOIS, serem públicos e se esta política de base de dados pública vai ao encontro dos princípios expostos no GDPR. É motivo para se perguntar, quais são os critérios de legitimidade na política do WHOIS para se aceder a esses dados? Será necessário os dados que identificam uma pessoa estarem expostos no WHOIS, ou deverão por outro lado, constar anónimos?

Foram dadas ideias, mencionados exemplos, para se usufruir de um WHOIS privado[26], para pelo menos dar-se a hipótese aos titulares dos dados, de no caso de desejarem ocultar as informações pessoais publicadas no registo WHOIS, o poderem fazer. Ora, segundo o princípio à limitação do tratamento[27], o titular dos dados pode exigir que o responsável pelo tratamento de dados limite a utilização dos seus dados recolhidos. Durante o período de limitação do tratamento, os dados só podem ser tratados com o consentimento do titular ou para efeitos de declaração, exercício ou defesa de um direito em processo judicial, dos direitos de outra pessoa singular ou coletiva ou, ainda, por motivos de interesse público. Outro ponto importante do GDPR a realçar relativamente a esta questão, é o direito ao esquecimento[28], o titular dos dados tem direito a que os mesmos sejam apagados e, consequentemente, deixem de ser objeto de tratamento. Olhando para estes dois direitos conferidos pelo GDPR, conclui-se a propósito do WHOIS que se deve avaliar as categorias de dados tratadas nesta ferramenta, rever as políticas de retenção de dados, rever as políticas de privacidade para incluir ao dados de perfil, criar e desenvolver políticas de acesso a dados pessoais e definir processos para assegurar o cumprimento das obrigações de "apagamento".

Com efeito, a ideia geral que saiu a este respeito da ICANN58 é de que a política utilizada no WHOIS deverá ser revista, sendo importante que os responsáveis pelo processamento de dados dos ccTLD´s tentem fazê-lo da forma o menos intrusiva possível.

26 *Como exemplo bloqueando o acesso a terceiros, através do login.*

27 *Art. 18º GDPR*

28 *Art. 17º GDPR*

A este respeito, surge o tema dos requisitos da Privacidade by *design*, ou "privacidade desde a conceção" que prevê a necessidade de incluir, em cada novo processo de tratamento de dados pessoais a ser implementado por uma organização, procedimentos que observem o cumprimento das regras de proteção de dados. O Regulamento indica expressamente a necessidade das organizações elaborarem avaliações de impacto ao nível da proteção de dados e manterem um registo sobre todas as atividades de tratamento de dados levadas a cabo. Estes procedimentos irão gerar custos de adaptação aos Registries, tanto pelo ajuste que se fará na gestão de dados, sistemas de acesso diferenciado, processos internos de coleta de dados, cópia de dados para outros lugares de armazenamento, bem como, na componente técnica, com, por exemplo, a realização de *backups*, no sentido de conferir uma maior segurança dos sistemas informáticos de proteção de dados.

Ora, concluindo, foi reiterada a importância dos Registries começarem a trabalhar desde já na implementação do GDPR avaliando eventuais impactos a nível administrativo, técnico e financeiro. Aconselhou-se especialmente, a seguir determinados passos na implementação do regulamento, começando pela identificação de todos requisitos do novo regime de proteção de dados, identificação dos dados pessoais geridos, análise detalhada dos riscos e por fim, pensar nas medidas para fazer face a esses riscos[29]. No fundo o que se pretende é um reforço do modelo *compliance*.

Levantou-se, por fim, a problemática de saber se existe conformidade da política da ICANN para Registries e Registrars, em relação ao cumprimento da legislação aplicável da união europeia. Isto porque os GeoTLDs europeus podem entrar em conflito com as obrigações previstas no contrato com a ICANN, na medida em que este estabelece cláusulas sobre o WHOIS, que são contraditórias com disposições previstas no GDPR. Por este motivo, o GeoTLDs solicitou à ICANN um forma de os desobrigar dessas regras, com fundamento na eventual violação de uma lei comunitária.

https://www.centr.org/library/library/external-event/centr-report-on-icann58.html

https://gacweb.icann.org/display/gacweb/Governmental+Advisory+Committee?preview=/27132037/44663677/GAC%20ICANN%2058%20Communique%20-%20Full%20-%2015mar17.pdf

29 *Identificação de tipos de processamento de dados que requerem private internet acess (análise destinada a identificar e minimizar os potenciais riscos para o não-cumprimento de disposições legais).*

ICANN | 58 • TECH DAY

Ao nível técnico o primeiro evento relevante foi o Tech Day, onde foram realizadas um conjunto de apresentações, de cariz técnico, e cujos principais resultados se passam a descrever.

Alexander Mayrhofer, do nic.at, apresentou uma ferramenta desenvolvida por este registry baseada no números de queries que observam nos servidores de nomes para um determinado domínio visando estabelecer um valor a que chamaram "DNS Magnitude" e que reflete a importância do domínio no universo dos domínios .AT.

O valor do "DNS Magnitude" para um domínio copia a escala de ritcher, que é usada para classificar os tremores de terra, e classifica assim a importância que um domínio tem dentro da zona .AT. Este valor é calculado tendo em conta uma fórmula que foi definida e afinada pelo nic.at e que dá mais importância a certos fatores como o número de queries observado.

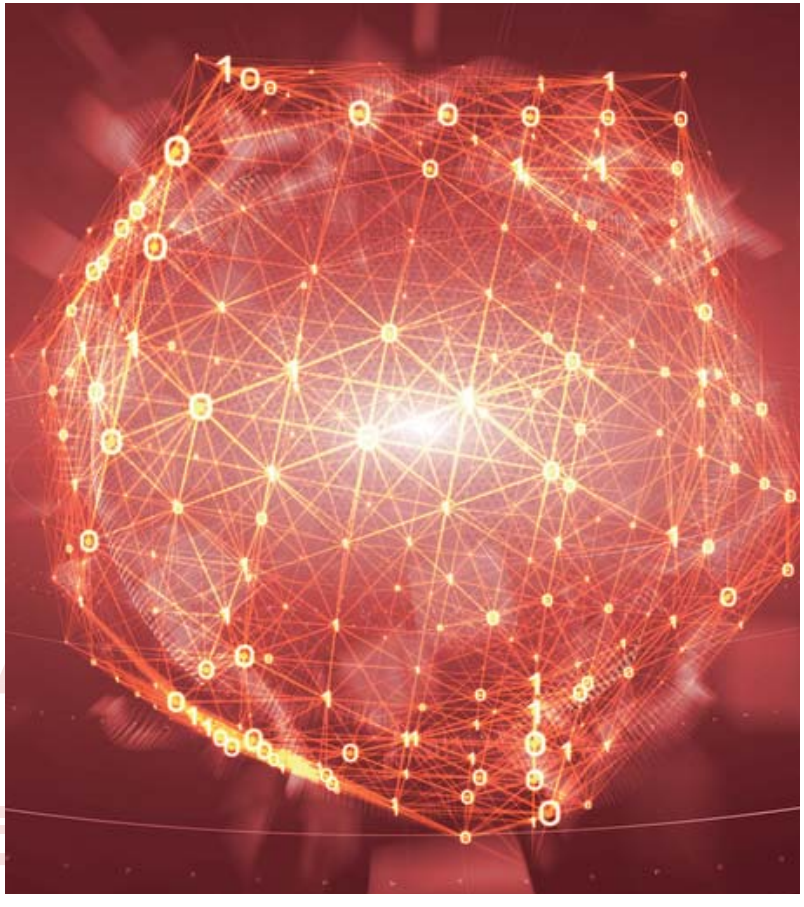
Como output desta ferramenta foi adicionado ao sistema de gestão do nic.at o valor da "DNS Magnitude" de cada domínio para que as pessoas internamente tenham noção da importância de cada domínio. Foi ainda correlacionado o valor da "DNS Magnitude" com a entrada de domínios em Pending-Delete ou possível entrada de domínios neste estado de forma a tentar precaver situações anómalas com domínios com a "DNS Magnitude" alta.

O DIFO apresentou o atual modelo de gestão técnico de sistemas e infra-estrutura do .DK e o atual modelo de desenvolvimento da aplicação de registo de domínios. A parte mais interessante desta apresentação focou-se na implementação que o .DK teve de fazer há cerca de 2 anos e que se prendeu com a validação de dados dos titulares dos domínios. Esta validação foi só implementada em domínios com titulares dinamarqueses e passa pelo envio de uma carta para as pessoas após o registo do domínio de forma a validar que aquela pessoa pediu efetivamente o registo do domínio.

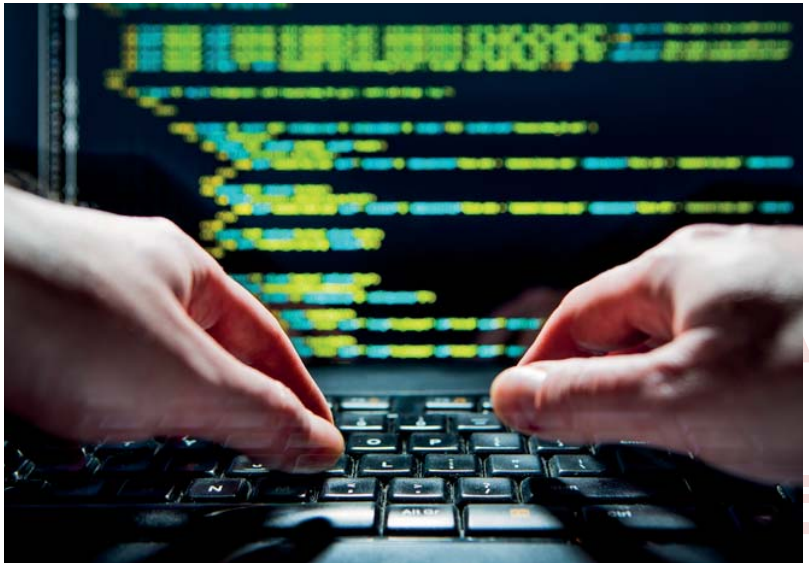
A terceira apresentação foi feita por um conjunto de organizações Holandesas e focou-se na medição de quanto da Internet usa encriptação para comunicar e no quanto a disponibilização de certificados que foi feita pela iniciativa Let's Encrypt (https://letsencrypt.org/) contribui para o aumento do uso de encriptação. Para estas estatísticas este estudo usou dados públicos disponibilizados pelos Web Browsers Mozilla Firefox e Google Chrome e pelo site de estatísticas Alexa.

O Registry russo que gere vários TLD's incluído o .RU e o .РФ (.RU em caracteres cirílicos apresentou o seu projeto de estatisticas o Statdom (http://statdom.ru/) que concentra as diversas estatísticas recolhidas pelo Registry. Tendo como base os dados obtidos por esta plataforma foi feita uma apresentação mais profunda do uso de certificados para encriptação de comunicações nos domínios desta entidade. Esta apresentação concluiu que o uso de certificados está a crescer nestes TLD's e que mais uma vez a plataforma Let's Encrypt (https://letsencrypt.org/) é um dos principais impulsionadores deste crescimento. Apesar deste aumento e das claras vantagens para a privacidade que este aumenta representa, ainda existem arestas por limar que se baseiam no facto de os certificados por vezes serem emitidos indevidamente e terem de usar mecanismos como o DANE para validar os certificados por uma segunda forma.

O .NZ realizou mais uma atualização da plataforma de reporting que criou baseada na análise dos dados de DNS que recebem. Esta plataforma de estatísticas já está bastante evoluída e já consegue providenciar dados individuais para cada domínio, caracterizando o tráfego e ranking do domínio. Foi ainda apresentado um sistema de monitorização e reporting do estado do DNS de cada domínio .NZ. Esta plataforma percorre regularmente a zona .NZ e reporta ao cliente caso haja algum problema na configuração por si indicada.



No passado mês de Outubro a Dyn, um dos principais providers de DNS a escala mundial, sofreu um ataque de larga escala ao seus sistemas que provocou uma interrupção de serviços a diversos sites de larga escala como por exemplo o twitter. Durante a sessão técnica a Dyn fez uma apresentação sobre o que se passou neste dia, de como o ataque tinha sido feito, que consequências tinha tido e como a empresa combateu o ataque. A parte mais relevante desta apresentação passou por demonstrar como o ataque foi feito, identificando como origem a bootnet Mirai que por esta altura provocou ataques em massa. Ao nível das conclusões de como combater um ataque deste tipo não existe uma solução mágica mas antes um conjunto de soluções que devem ser aplicados por vários players e que devem, com isso, contribuir para criar uma internet mais segura.



O DNS Belgium, o registry do .be, focou a sua apresentação na mudança do seu sistema de registo para a cloud da Amazon a AWS. A principal razão para esta alteração foi o facto de o hardware ser algo complicado de gerir e que acaba por alocar muito tempo às equipas internas. Ao migrar para a cloud a equipa técnica pode-se focar mais no desenvolvimento da ferramenta de registo e deixar de se preocupar com questões complexas de gestão de contratos de hardware. Esta mudança não é pacífica nem é bem vista por toda a comunidade face aos problemas conhecidos que a cloud tem ao nível da segurança e independência face a terceiros, que são questões fulcrais para um TLD. Também foram demonstrados problemas ao nível da disponibilidade, uma vez que uma dos principais vantagens que são vendidas da cloud é a alta disponibilidade geográfica, mas a migração do .BE demonstrou que neste momento ainda não atingiram este ponto uma vez que os seus sistemas ainda dependem de uma localização geográfica, sendo um dos pontos futuros a criação de um segundo sistema para se atingir a verdadeira alta disponibilidade. No geral a DNS Belgium considerou a migração positiva apesar das limitações que já foram faladas e dos trabalhos que ainda necessitam de ser feitos.

A apresentação seguinte foi feita pela NL Net Labs e foi mais um update ao projeto DPRIVE que pretende criar canais de comunicação segura entre os clientes e os resolvers de forma a que não seja possível interceptar e manipular as perguntas de um cliente. A implementação deste projeto segue a bom ritmo já havendo a total especificação da implementação e já havendo algum software compatível com a mesma. Seguem-se a fase de massificação da solução por todo o software de DNS e por fim a

implementação por toda a comunidade da internet que se espera que seja o ponto mais difícil.

A CIRA focou-se no sistema de registo desenvolvido pelos canadianos e em especial nas funcionalidades de BI (Business Inteligence) que adicionaram ao sistema. A ferramenta de BI é baseada no sistema open source Pantaho e tem como base as várias componentes que integram o sistema de registo, conseguindo extrair diversos relatórios os quais podem ser configurados pelos utilizadores.

A última apresentação foi feita em conjunto entre o FBI e a Europol e centrou-se numa iniciativa de 2016 envolvendo as duas entidades e que acabou por desmantelar uma rede internacional que se dedicava a "vender" pishing. Esta organização Ucraniana usava DGA (Domain Generation Algorithms) para o envio de pishing para as pessoas e desta forma obter um retorno financeiro. Numa iniciativa em larga escala o FBI e a Europol com a colaboração com diversos TLD's, desmantelaram a rede e acabaram com a proliferação de emails falsos. De notar que o papel extremamente importante que os TLD's tiveram nesta iniciativa de forma a bloquear o registo de mais domínios maliciosos e a parar a atividade da rede de forma conciliada, conseguindo que os agentes maliciosos não fossem alertados a priori para o facto de que algo estava a ocorrer.

Na quarta-feira realizou-se mais um workshop de DNSSEC integrado no ICANN. Estes workshop seguem a evolução da penetração do DNSSEC na comunidade e alertam para a necessidade de implementação deste protocolo.

Na introdução a sessão foi feito uma atualização ao números da penetração de DNSSEC nos TLD's. A este nível continua a ser vista uma evolução ao nível dos TLD's assinados mas tem-se verificado um decréscimo no número de novos devido ao facto de não existirem muitos em falta.

Seguiu-se um painel de discussão sobre as últimas atualizações em alguns ccTLD's Europeus, nomeadamente no .DK, .DE, .AT e .CZ. As questões mais relevantes discutidas nesta sessão foram o início da inclusão do novo algoritmo para chaves de DNSSEC, o Edwards-curve Digital Security Algorithm (EdDSA), a evolução positiva que os domínios com DNSSEC têm estado a ter e o início da descontinuação de Assinaturas do tipo SHA1.

A segunda parte da Workshop começou por mais uma sessão de consciencialização e alerta para o facto de KSK da root ir mudar no dia 18 de Outubro e seguiu com uma sessão em que se falou dos possíveis problemas que poderiam existir para os operadores que já fazem validação de DNSSEC com esta alteração.

Os operadores convidados para esta sessão são alguns dos que já fazem validação DNSSEC e portanto estão bastante conscientes dos possíveis problemas e de soluções para mitigar a existência de problemas na validação DNSSEC devido a alteração da chave da root. No entanto, nesta sessão, alertou-se para o facto dos

operadores que não são tão ativos a este nível ou que têm uma menor consciencialização do problema poderem começar a sofrer problemas devido a rotação das chaves e não estarem preparados para lidarem com este. Para resolver esta situação foi sugerido que as entidades e pessoas que têm consciência do problema devem alertar a restante comunidade do país para que a rotação de chaves ocorra de uma forma suave.

Seguiu-se uma sessão onde foi apresentada mais uma aplicação de DNSSEC, na qual para estabelecer túneis IPSEC a chave pública destes túneis é publicada no DNS e validada usando DNSSEC. Sem este mecanismo de validação o utilizador tem de confiar na chave do túnel sem os poder validar.

Houve ainda uma apresentação na qual foi efetuada uma medição da adoção de chaves tipo ECDSA nas implementações de DNSSEC pelo mundo. A conclusão a que se chegou foi que nos últimos tempos estavam a ser vistos mais chaves deste tipo e que o principal responsável por esta descolagem no uso deste tipo de cifra é a CloudFlare que implementa nos domínios por si alojados este tipo de cifra por defeito.

A penúltima apresentação do workshop focou-se na divulgação de uma iniciativa, o TES (Trusted Email Service). Esta iniciativa visa promover a troca de emails seguros, situação com bastante debilidade a nível mundial, e tem como base o uso de DANE+DNSSEC para validar os certificados usados pelos servidores de email para trocarem a informação. Por último a iniciativa apresentou uma estatística atual do uso de DANE+DNSSEC nos servidores de email das grandes empresas de telecomunicações para validação e para já a o resultado é muito mau havendo poucas entidades a fazer esta validação, mas existe a intenção de continuar a sensibilizar as entidades para a necessidade deste tipo de validação.

Por último, neste fórum foi feita uma apresentação do SMILLA que é um projeto que pretende estender a autenticação baseada em SMIME usando validação por DNSSEC. O SMIME permite a um utilizador enviar emails assinados ou encriptados mas mais uma vez a parte pública da chave de encriptação usada tem de ser enviada no email e não existe nenhuma forma de validar a sua autenticidade. Desta forma o SMILLA tenta combater este deficiência do SMIME colocando no DNS a chave pública dos certificados SMIME de cada cliente para esta poder ser usada por terceiros usando o DNS. Este projeto está muito no início mas a ideia agrada à comunidade já que é mais uma aplicação para o DNSSEC.

Destaca-se por fim um tema técnico que esteve bastante em voga nesta ICANN e que foi alvo de algumas conversas e work-shop's, a rotação da KSK DNSSEC da root.

Esta alteração irá começar em julho deste ano com a publicação da nova chave e terá o seu ponto forte a 11 de Outubro de 2017, altura em que esta nova chave irá assinar pela primeira vez a zona root.

No geral a comunidade sente-se confiante que esta alteração será pacífica. Não obstante este facto, está a ser feito um esforço de comunicação e sensibilização para que a alteração corra sem problemas, sobretudo para os operadores da rede que não são tão ativos e tão atentos a questões relativas a DNS.

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

ASSOCIAÇÃO dns.pt

Produção: março 2017
Grafismo: dns.pt