



**Sessão de Debate organizada pelas associações:
APDSI e ISOC PT, com apoio institucional da Universidade Aberta**

Data — 25 de Maio de 2022 - 17h00 — Participação presencial e também online

Registo obrigatório — https://pt.surveymonkey.com/r/Internet_Geopolitica

Local — Salão nobre da Universidade Aberta, Rua da Escola Politécnica 147, Lisboa

Línguas de trabalho — Português e Inglês

Organizadores — APDSI (<https://apdsi.pt>) e ISOC Portugal (<https://isoc.pt>)

A guerra na Ucrânia está a ser acompanhada de pressões políticas que poderão levar, se não forem combatidas, a que a visibilidade dos serviços disponíveis na Internet se torne totalmente dependente da região ou bloco geopolítico em que cada utilizador acede à “rede das redes”. Serão estes acontecimentos pronúncio de que a Internet se vai particionar em diferentes redes por via das fricções e conflitos (económicos, políticos ou mesmo armados) entre blocos? Ou na verdade esta situação não passa de uma manifestação de uma realidade pré-existente, inevitável e que se manifesta continuamente, apesar de com intensidade variável?

O termo *Splinternet* é usado para designar uma Internet fragmentada onde a visibilidade de outras redes e serviços está sujeita a filtros introduzidos por razões económicas, políticas ou geopolíticas. Importa, no entanto, não esquecer que o termo *Splinternet* não se aplica aos filtros aplicados para combater o banditismo e o terrorismo. Tecnicamente, como defendido pelos organismos de governação dos protocolos, nomes e endereços da Internet (IETF, ICANN e Regional Registries), a possibilidade de comunicação entre equipamentos ligados a diferentes áreas da mesma é, teoricamente, sempre possível. Esses organismos de governação recusam contribuir para a *Splinternet*.

No entanto, é realista acreditar que a Internet acabou com a soberania dos Estados sobre os seus territórios? Ou seja, que a soberania tradicional, geralmente com um âmbito territorial, não tenha hoje em dia uma nova emanção que se pode designar por ciber soberania? A *Splinternet* é algo novo a combater vigorosamente, ou sempre existiu e é inevitável? Temos de a recusar com todas as nossas forças, ou temos de a aceitar e encontrar formas, por exemplo através de tratados, de minorar os seus inconvenientes?

Para uma análise ainda preliminar do que é a *Splinternet* e de como se podem minorar os seus impactos negativos, a Associação Portuguesa para o Desenvolvimento da Sociedade da Informação (APDSI) e o Capítulo Português da Internet Society (ISOC PT), com o apoio da Universidade Aberta, promovem esta sessão de debate.

Programa

17:00 – 17:05 Recepção dos participantes

17:05 – 17:10 Abertura

- **Universidade Aberta**
- **Maria Helena Monteiro** – Presidente da Direção da APDSI
- **Nuno Guimarães** – Presidente da Direção do ISOC PT

17:10 – 18:10 Apresentações pelos oradores convidados

Moderador: **Nuno Guimarães**

- **Andrea Becalli** - Senior Director for Stakeholder Engagement at Internet Corporation for Assigned Names and Numbers (ICANN)
- **David Frautschy Heredia** - Senior Director for European Government and Regulatory Affairs at Internet Society (ISOC)
- **José Legatheaux Martins** - Professor jubilado da FCT/UNL e ex-presidente do ISOC Portugal
- **Victor Angelo** - Ex Secretário Geral Adjunto das Nações Unidas

18:10 – 19:00 Debate com a participação da assistência

Oradores

Enquadramento do debate

A invasão da Ucrânia pela Rússia teve um impacto importante ao nível do *core* da Internet, mas também nos serviços de informação cujo funcionamento é suportado pela “rede de redes”. De facto, esta guerra introduziu vários bloqueios nas comunicações dos blocos geopolíticos nela envolvidos.

Adicionalmente, logo após a invasão, a Ucrânia solicitou ao ICANN que os domínios .RU e .SU fossem banidos da Internet, e solicitou ao RIPE que os endereços IP afectados a redes russas lhes fossem retirados. Felizmente, ambos os pedidos foram firmemente descartados pois não faz parte dos objetivos da ICANN ou do RIPE sujeitarem a gestão da Internet a constrangimentos e conflitos geo-políticos, nem privar populações do acesso à Internet devido a conflitos entre os seus governos. Tal como o ar que respiramos não reconhece fronteiras, também não devem ser impostas fronteiras geopolíticas aos nomes e aos endereços usados na Internet.

Serão estes acontecimentos pronuncio de que a Internet se vai particionar em diferentes redes por via das fricções e conflitos (económicos, políticos ou mesmo armados) entre blocos? Ou na verdade esta situação não passa de uma manifestação de uma realidade pré-existente, inevitável e que se manifesta continuamente, apesar de com intensidade variável?

O termo *Splinternet* é usado para designar uma Internet fragmentada onde a visibilidade de outras redes e serviços está sujeita a filtros introduzidos por razões económicas, políticas ou geopolíticas. Importa, no entanto, não esquecer que o termo *Splinternet* não se aplica aos filtros aplicados para combater o banditismo e o terrorismo. Tecnicamente, como defendido pelos organismos de governação dos protocolos, nomes e endereços da Internet (IETF, ICANN e Regional Registries), a possibilidade de comunicação entre equipamentos ligados a

diferentes áreas da mesma é, teoricamente, sempre possível. Esses organismos de governação recusam contribuir para a *Splinternet*.

No entanto, é realista acreditar que a Internet acabou com a soberania dos Estados sobre os seus territórios? Ou seja, que a soberania tradicional, geralmente com um âmbito territorial, não tenha hoje em dia uma nova emanção que se pode designar por *ciber soberania*?

Mesmo que a conectividade entre todas as redes fosse global, universal e sem filtros, isso acaba com a competição económica, política e militar? Será que universalidade e globalidade da rede torna a concorrência económica e política automaticamente saudável e independente dos poderes em jogo? Não, tal como para o movimento de bens, pessoas, ideias, informações, etc. só com tratados negociados entre Estados se podem manter formas de competição e coexistência pacíficas. Idealmente, esses tratados devem ser de facto respeitados e também serem independentes do poder relativo entre Estados.

Em caso de conflitos económicos, políticos ou militares, não é legítimo os Estados e os respetivos Governos usarem as armas de que dispõem para defender os interesses da maioria dos seus cidadãos que representam — mesmo que essa representatividade seja apenas admitida para efeitos diplomáticos? Será que os Governos não têm de tomar medidas para defenderem as suas infra-estruturas críticas, incluindo nas mesmas as ciber infra (e super) estruturas, da qual depende o funcionamento das Sociedades porque são responsáveis?

De facto, provavelmente a Splinternet é uma realidade inevitável que existe de facto, e que se manifesta de formas mais dissimuladas, como no assim designado Ocidente, ou mais brutais, como na Rússia e na China, ou ainda com imensas variantes entre estes dois extremos em muitas outras geografias. Pensar que a Internet pode ser imune à expressão dos interesses económicos, políticos e de defesa militar dos diferentes países e blocos geopolíticos parece ser uma hipótese pouco realista e talvez ingénua.

Reconhecida a inevitabilidade da existência da ciber soberania, pois a mesma tem base na praxis e teoria da coexistência entre as nações do mundo, quais os limites a que essa soberania deve estar sujeita?

Partindo desta visão, de que forma será possível uma ciber coexistência pacífica entre blocos, permitindo a defesa dos direitos e dos interesses das populações que os integram? Não sendo a Internet imune à realidade dos interesses dos diferentes países e blocos, que tratados podem contribuir para manter a fluidez das comunicações e evitar o seu uso como arma de agressão económica, política ou militar? Será que os tratados de comércio, ou de coexistência política e militar como a carta das Nações Unidas, ou ainda os tratados de defesa dos direitos dos civis em tempo de guerra, são suficientes? Ou serão necessários outros adaptados à ciber soberania?

Apoio institucional



Organização

