

European Regional Bureau Newsletter



11 August – 18 August 2017

<http://www.Internetsociety.org/what-we-do/where-we-work/europe>

Frédéric Donck (ERB)

Internet Access

UK: Mayor of London announced plans to boost digital connectivity

- On August 10, the Mayor of London Sadiq Khan [announced](#) plans to tackle London's connectivity “not-spots” and to deliver connectivity in the city underground.
- A City Hall summit – the Digital Connectivity Funding Forum – will be organised to gather local authorities and encourage them to apply for the Government’s Digital Infrastructure Funding.
- The Mayor stated Londoners and businesses “need fast and reliable digital connections in order to remain competitive in the global economy.”

EU: Commission approved German aid scheme to support high speed Internet solutions for rural areas

- On August 11, the European Commission approved a €3 billion government funded broadband service programme for rural areas in Germany, saying it does not break state aid competition rules. The Commission has thus [approved](#) the three virtual unbundled local access (VULA) products proposed by Deutsche Telekom, DNS:Net and NetCologne, allowing for the use of vectoring technology in state-funded high speed broadband networks across the country.
- In 2015, the Commission approved the [state aid broadband programme](#) aimed at boosting investments in high speed broadband infrastructures in the country using vectoring technology, on the condition that Germany offered VULA products “to replace the physical access lost caused by the use of vectoring technology.”
- Vectoring technology increases broadband speed over existing copper network compared to levels normally achieved via very high speed digital subscriber lines (VDSL). However, competitors could potentially no longer be able to have access to individual copper lines. The introduction of VULA can compensate the side effects of vectoring technology and ensure open access to the network.

EU: Digital Commissioner answers parliamentary question on WiFi4EU initiative

- Answering a [parliamentary written question](#), the European Commissioner in charge of the Digital agenda Mariya Gabriel [said](#) on August 17 that free wireless connectivity provided in public areas, the [WiFi4EU](#) scheme, “contributes to bridging the digital divide.”

- Commissioner Gabriel also specified that the initiative will “exclude projects that duplicate already existing private or public offers with similar characteristics (including quality of service) in the same area.” This will ensure that free wireless connectivity will be provided to the most remote regions and rural areas in Europe.
- The budget of the WiFi4EU is €120 million for the next two years to support the installation of Wi-Fi in the centres of community life across the EU.

Trust

UK: MI5 former head warns against crackdown on encrypted messaging apps

- During an interview given to [BBC Radio 4](#), the former chief of the British intelligence service, Jonathan Evans, declared he “would not support a clampdown on use of encryption” in the fight against terrorism. Mr Evans stressed the importance of implementing measures to strengthen cybersecurity without weakening encryption.
- His comments came after Home Secretary Amber Rudd [recently claimed](#) that “real people do not need end-to-end encryption in messaging apps”.

Scotland: Scottish Parliament hit by prolonged “brute-force” cyberattack

- On August 15, the Scottish Parliament was targeted by a brute-force cyberattack (i.e. involving hackers repeatedly attempting to crack passwords) aimed at users’ e-mail accounts, similar to that which hit Westminster in June this year.
- [According to Clerk and Chief Executive of the Scottish Parliament Sir Paul Grice](#), cyber defence was strengthened and the assault has not breached the Parliament’s IT systems.
- The Parliament’s Business Information Technology Office has been working with the UK’s National Cyber Security Centre to implement additional cybersecurity measures and understand the origin of the attack.

UK: Cybersecurity sectoral analysis survey open until the end of August

- On August 15, the UK Department for Digital, Culture, Media and Sport (DCMS) launched an [open consultation](#) to collect data on the country’s cybersecurity industry.
- The DCMS commissioned RSM’s Economic Consulting team (PACEC) and the Centre for Secure Information Technologies (CSIT) at Queen’s University Belfast, to provide statistics about the sector’s size, scale and future opportunities.
- The results of the consultation will help the Government to better understand how to support the sector’s growth.
- The survey is open until August 31.

EU: business organisations call for effective cybersecurity rules

- Ahead of the EU Cybersecurity Strategy review (expected in September 2017), numerous chambers of commerce and business associations called on the European Commission to develop effective rules “to raise cyber defences and realise the potential of the Internet of Things (IoT).”
- In a [joint letter](#) sent to European Commission Vice-President Andrus Ansip and Digital Commissioner Mariya Gabriel, the organisations propose to focus on six “principles”. These include the need to “resist the urge to regulate the IoT prematurely”; to develop globally recognised standards and best practices; and to introduce an EU “trust label”.
- The business groups also suggest to facilitate cyber information sharing and increase awareness on cybersecurity among the public.
- Among others, the signatories include the US Chamber of Commerce, the confederations of industry of both Denmark and the Czech Republic, and EurElectric,

the sector association which represents the common interests of the electricity industry at a European level.

UK: NHS Digital and Microsoft signed cybersecurity deal

- NHS Digital, the UK National Health Service's provider of information, data and IT systems, signed a custom support [agreement](#) with Microsoft in an effort to improve its cybersecurity capability.
- From now until mid-2018, Microsoft will provide for the detection of cyber threats that target IT devices relying on outdated operating systems. All existing Windows devices operating on Windows XP, Windows Server 2003 and SQL 2005 will thus be updated by the end of the agreement.
- The deal comes three months after [numerous UK hospitals](#) were hit by the WannaCry malware attack as part of the [government's plan](#) to bolster cybersecurity within the NHS.