31 January 2018

Synopsis

Scroll to read full summaries with links to news articles.

China has attempted to gain more control over the **internet** by announcing this week that local and foreign companies can only use Government approved **software** to access the global internet.

According to security experts, the technology firm **Intel** warned the **Chinese Government** about their security flawed chips before the **United States Government**, giving Beijing the potential opportunity to exploit them.

Technology company **Google** is expanding its presence in the **Asia-Pacific** region after it announced it had secured a deal with Taiwanese Handset Maker HTC. **Taiwan** will be the largest engineering site for the technology giant.

Sir **Julian King**, European Commissioner for the Security Union urged all European countries to use the same **cybersecurity** processes and products to ensure 'uniformity of efficacy.'

France have announced they are developing a five-year **cybersecurity** strategy which will see an increase in funding and an extra eight-hundred police appointed to focus solely on cyber.

The **European Union** have published guidelines to help countries prepare for the **General Data Protection Regulation** rules being implemented in four months. They also announced an extra €2 million to help authorities guide businesses.

The **FCC**, wireless companies and several lawmakers have announced that they would oppose the **US** President's plan to build a Government owned **5G** generation mobile network to mitigate **privacy threats** from **China**.

California signed a Bill this week to enforce **Internet service providers** to adhere to the **net neutrality** rules that the **Federal Communications Commission** repealed last month. **New York** became the second State to enforce net neutrality via an executive order.

1

Mayor **Sam Liccardo** has resigned as a member of the **Federal Communications Commission** Advisory Committee, which focuses on **broadband** deployment, on grounds that it only lobbies for major internet companies.

The **UK** Government revealed that ninety-five percent of its premises have access to superfast **broadband** compared to just twenty-one percent in **Nigeria**.

French newspaper, **Le Monde**, has reported that **China** used the **Africa** Union's IT division to '**spy**' on the nations in the Union. China was the one to finance and build the building and so had access to the system.

Penalties are set to be rolled out to **telecom operators** that mask international telephone calls, The **Nigerian Communications Commission** hope this will reduce **call masking**.

During a joint press conference, Secretary General for NATO **Jens Stoltenberg** announced that a new **NATO cyber academy** was being built in **Portugal** to discover the next generation of cyber experts.

Disclaimer: Please note that this monitor is a summary of news sources and does not reflect the official views of IEEE.

For more information, visit the IEEE Internet Initiative website, and see *IEEE Global Internet Policy Monitor* past issues. Join IEEE Collabratec™ Internet Technology Policy Community discussions related to internet policy issues and to collaborate with other members of the global technical and policy communities.

IEEE Global Internet Policy Monitor

31 January 2018

Table of Contents

Europe

Internet governance

29.01.18

SC Media

[Data Protection Day: EC issues GDPR guidance](#)

The European Union published guidelines to help countries prepare for the General Data Protection Regulation rules being implemented in four months. They also announced an extra €2 million to help authorities guide businesses.

"With just under four months to go before the General Data Protection Regulation (GDPR) takes effect, the European Commission (EC) published guidance last week, meant to help organisations apply the new rules to their businesses."

"Ahead of Sunday's Data Protection Day (28/1/2018), with just under four months to go before the General Data Protection Regulation (GDPR) takes effect, the European Commission (EC) published guidance last Thursday meant to help organisations apply the new rules to their businesses."

Cybersecurity

26.01.18

SC Media

[FIC 2018: Pan-European cyber-security certification urged](#)

Sir Julian King, European Commissioner for the Security Union urged all European countries to use the same cybersecurity processes and products to ensure 'uniformity of efficacy.'

"During the 10th Forum International de la Cybersecurity in Lille, France, this week - calls were made for pan-European certification of cyber-security products to ensure uniformity of efficacy, with help for less developed markets."

"Sir Julian King, commissioner for the Security Union, European Commission, told delegates at the Forum International de la Cybersecurity this week how 2017 was the year that many finally became aware of cyber-security due to the huge attacks which were able to proliferate fast and overcome borders - with WannaCry in particular."

26.01.18

SC Media

[FIC 2018: Defending France - 5-year plan to operate on a larger scale](#)

France have announced they are developing a five-year cybersecurity strategy which will see an increase in funding and an extra eight-hundred police appointed to focus solely on cyber.

"Gérard Collomb Ministre de l'Intérieur de France: France is currently developing its five-year strategy to fight cyber-crime on a large scale. The new ambition is to protect France. 800 extra police dedicated to cyber. Increased spend."

"Gérard Collomb Ministre de l'Intérieur de France began his presentation by describing cyber-security as one of the main challenges of the 21st century."

29.01.18

SC Media

[Failure to comply with U.K. gov't directive to bolster cybersecurity, infrastructure firms could face stiff fines](#)

The UK Government have warned that British industries running critical infrastructure including water, energy, transport and health firms could face fines of up to £17 million if they fail to make their business cyber resilient.

"The British government Sunday warned the heads of firms in the country's most critical industries to bolster their cybersecurity efforts to avoid fines."

"If they don't make the necessary moves to ratchet up cybersecurity and invest in proper safeguards, the newly appointed special-sector regulators could fine energy, transport, water and health companies as much as £17 million, according to a release."

Privacy

26.01.18

Cisco

[Privacy Maturity Benchmark Study](#)

According to report by technology company Cisco the most 'privacy-immature companies suffered from seventy four percent of cyber losses over £500,000 compared to thirty nine percent of 'mature' companies.

"The General Data Protection Regulation (GDPR) will become fully enforceable on May 25, 2018. Many organizations are rightly investing in resources and processes to meet the GDPR standards and avoid significant fines and other penalties."

"In addition, the many data breaches that exposed the personal information of millions of customers have made organizations increasingly concerned about the products they buy and with whom they partner."

26.01.18

SC Media

[£20 million Institute of Coding to be built, PM announces at Davos](#)

The UK Prime Minister Theresa May announced that the Government would give industry experts, businesses and sixty universities, £20 million to create an Institute of Coding, aimed at improving higher-level digital skills.

"A consortium of more than 60 universities, industry experts and businesses is set to receive £20 million to create the Institute of Coding to help create the next generation of digital specialists, according to Prime Minister Theresa May."

"May was speaking at the World Economic Forum in Davos, Switzerland, about how the Institute of Coding is a key part of the plans of the government to drive up digital skills through its Industrial Strategy, helping to equip people of all ages with the skills they need for the future."

Internet Inclusion

26.01.18

NATO

[Joint press conference](#)

During a joint press conference General Jens Stoltenberg announced a new NATO art cyber academy being built in Portugal, to discover the next generation of cyber experts.

"Thank you so much. And it's a great honour to be here and to once again meet with you. We have met many many times, but this is actually our first meeting in Lisbon. And for me it is a great honour to be here because Portugal is such a key Ally in our Alliance."

"Portugal makes NATO more secure - on land, at sea, in the air and also in cyber-space. We are very grateful for your many contributions."

30.01.18

Computer Weekly

[UK government signs Tech Talent Charter diversity initiative](#)

The UK Government has signed the Tech Talent Charter to address the gender diversity gap in the technology industry. Those who sign the Charter commit to including women on shortlists and collecting data for an annual diversity report.

"The government has committed to sign the diversity initiative Tech Talent Charter in an aim to close the gender diversity gap in the technology industry."

"The UK government has agreed to sign diversity initiative Tech Talent Charter (TCC) to address the lack of gender diversity in the technology industry."

31.01.18

The Guardian Nigeria

[UK hits 95% broadband penetration as Nigeria struggles at 21%](#)

The UK Government revealed that ninety-five percent of its premises have access to superfast broadband compared to just twenty-one percent in Nigeria. The Nigeria Communications Commission has been accused of not following the National Broadband Plan.

"Though, the Nigerian Communications Commission (NCC), has assured that Nigeria would meet and surpass the 30 per cent penetration target, however, stakeholders are sort of skeptical.

"They based their argument on the National Broadband Plan (NBP), which is not been followed adequately."

United States of America

Internet governance

25.01.18

Ars Technica

[Mayor quits FCC committee, says it favors ISPs over the public interest](#)

California Mayor Sam Liccardo has resigned as a member of the Federal Communications Commission advisory committee, which focuses on broadband deployment, on grounds that it only lobbies for major internet companies.

"A broadband deployment advisory group organized by the Federal Communications Commission is trying to make it harder for cities and towns to build and operate their own Internet services."

"The Broadband Deployment Advisory Committee (BDAC) was set up by the FCC last year and is now releasing draft versions of its recommendations. One member—the mayor of San Jose, California—quit the group today out of frustration that the recommendations favor the interests of private industry over municipalities."

25.01.18

Ars Technica

[Net neutrality will be enforced in New York under orders from governor](#)

New York has become the second state to enforce net neutrality in defiance of the American telecom regulator the Federal Communications Commission's decision to remove these rules last month.

"New York has become the second state to enforce net neutrality with an executive order that prevents ISPs from obtaining state contracts unless they follow net neutrality principles."

"New York Governor Andrew Cuomo signed the executive order yesterday, days after Montana Governor Steve Bullock did the same. The states are challenging the Federal Communications Commission, which repealed its own net neutrality rules and preempted states from imposing similar ones."

29.01.18

CNN

[Trump team idea to nationalize 5G network to counter China is rejected](#)

The FCC, wireless companies and several lawmakers have announced that they would oppose the US President's plan to build a Government owned 5G generation mobile network to mitigate privacy threats from China.

"The top U.S. communications regulator, wireless companies and some lawmakers oppose an idea by members of President Donald Trump's national security team for the government to build a 5G wireless network to counter China spying on phone calls."

"The Trump administration has taken a harder line with China on policies initiated by predecessor President Barack Obama on issues ranging from Beijing's role in restraining North Korea to Chinese efforts to acquire U.S. strategic industries."

29.01.19

South China Morning Post

[Trump's rush to build a national 5G network may backfire, give China the technological edge](#)

Analysts have warned that the US President's plan to build a Government-owned 5G network in a bid to counter the threat of China spying on the country could slow down the countries deployment of the mobile technology.

"The programme drawn up by US President Donald Trump's national security team could backfire and slow down 5G deployment in America, analysts said."

"A plan by US President Donald Trump's national security team to build a government-owned 5G network, designed to counter the threat of China spying on calls, is seen as reflecting the mistrust by Washington towards Chinese hi-tech capabilities."

30.01.18

Ars Technica

[California Senate defies FCC, approves net neutrality law](#)

The California State Senate approved a Bill that will enforce Internet service providers to adhere to net neutrality rules that the Federal Communications Commission repealed last month.

"New York has become the second state to enforce net neutrality with an executive order that prevents ISPs from obtaining state contracts unless they follow net neutrality principles."

"New York Governor Andrew Cuomo signed the executive order yesterday, days after Montana Governor Steve Bullock did the same. The states are challenging the Federal Communications Commission, which repealed its own net neutrality rules and preempted states from imposing similar ones."

Cybersecurity

26.01.18

SC Media

[**Global tech firms let Russian defence agency peek at source code for flaws**](#)

American and European tech companies, McAfee, Symantec, Micro Focus and SAP have given the Russian Defence Agency their consent to uncover vulnerabilities in their systems.

A handful of tech companies have given a Russian defence agency the opportunity to sort the source code of their software, to uncover vulnerabilities that the Russians say could be exploited by bad actors.

McAfee, Symantec, Micro Focus and SAP all have submitted to the practice, sparking concern at the Pentagon and among lawmakers, according to a Reuters review of both US defence contracts and Russian regulatory requirements.

31.01.18

Department of Defence

[**DoD's Network Defense Headquarters Achieves Full Operational Capability**](#)

The United States have announced that the US Cyber Command, the Pentagon's digital warfare organisation that protects the Defence Departments 15,000 networks, is now fully operational.

"The U.S. Cyber Command component responsible for securing, operating and defending the Defense Department's complex infrastructure of roughly 15,000 networks with 3 million users has achieved full operational capability."

"Joint Force Headquarters Department of Defense Information Network reached the milestone after three years of building capacity and capability to secure, operate and defend the DoDIN, a global network enabling military operations across all warfighting domains."

Privacy

26.01.18

Cisco

[Privacy Maturity Benchmark Study](#)

According to a report by technology company Cisco, the most 'privacy-immature' companies suffered from seventy four percent of cyber losses over £500,000 compared to thirty nine percent of 'mature' companies.

"The General Data Protection Regulation (GDPR) will become fully enforceable on May 25, 2018. Many organizations are rightly investing in resources and processes to meet the GDPR standards and avoid significant fines and other penalties."

"In addition, the many data breaches that exposed the personal information of millions of customers have made organizations increasingly concerned about the products they buy and with whom they partner. Customers are asking more questions during the buying cycle about how data is captured, transferred, stored, and deleted. In this study, Cisco shares insights on how data privacy concerns are impacting the buying cycle."

28.01.18

The Hill

[Intel told Chinese firms about chip flaw before US govt: report](#)

According to security experts, the technology firm Intel warned the Chinese Government about their security flawed chips before the United States Government, giving Beijing the potential opportunity to exploit them.

"Intel Corporation warned a handful of customers, including several Chinese technology firms, about security flaws within its processor chips before the U.S. government, The Wall Street Journal reported Sunday."

"Security experts told the newspaper that the decision could have allowed Chinese tech companies to flag the vulnerabilities to Beijing, giving the Chinese government an opportunity to exploit them."

Internet Inclusion

30.01.18

Channel NewsAsia

[Google closes HTC deal; Taiwan now largest engineering site in Asia Pacific](#)

Technology company Google is expanding its presence in the Asia- Pacific region after it announced it had secured a deal with Taiwanese Handset Maker HTC. Taiwan will be the largest engineering site for the technology giant.

"Google on Tuesday (Jan 30) announced it has officially closed its deal with Taiwanese handset maker HTC."

"In a blog post by the company's senior vice president for Hardware Rick Osterloh, he said it is welcoming an "incredibly talented team" who have decades of experience "achieving a series of firsts" in the smartphone industry. These include bringing the first 3G smartphone to market in 2005, the first touch-centric phone in 2007 and the first all-metal unibody phone in 2013, he explained."

Pan-Asia

Internet governance

29.01.19

South China Morning Post

[Trump's rush to build a national 5G network may backfire, give China the technological edge](#)

Analysts have warned that the US President's plan to build a Government-owned 5G network in a bid to counter the threat of China spying on the country could slow down the countries deployment of the mobile technology.

"The programme drawn up by US President Donald Trump's national security team could backfire and slow down 5G deployment in America, analysts said."

"A plan by US President Donald Trump's national security team to build a government-owned 5G network, designed to counter the threat of China spying on calls, is seen as reflecting the mistrust by Washington towards Chinese hi-tech capabilities."

29.01.18

CNN

[Trump team idea to nationalize 5G network to counter China is rejected](#)

The FCC, wireless companies and several lawmakers have announced that they would oppose the US President's plan to build a Government owned 5G generation mobile network to mitigate privacy threats from China.

"The top U.S. communications regulator, wireless companies and some lawmakers oppose an idea by members of President Donald Trump's national security team for the government to build a 5G wireless network to counter China spying on phone calls."

"The Trump administration has taken a harder line with China on policies initiated by predecessor President Barack Obama on issues ranging from Beijing's role in restraining North Korea to Chinese efforts to acquire U.S. strategic industries."

30.01.18

Channel NewsAsia

[China directs users to approved VPNs as firewall tightens](#)

China has attempted to gain more control over the internet by announcing this week that local and foreign companies can only use Government approved software to access the global internet.

"China vowed on Tuesday (Jan 30) to force both local and foreign companies and individuals to use only government-approved software to access the global internet, as overseas firms fear losing unrestricted online services under an impending deadline."

"International companies and individuals have been fretting for months over whether Beijing would enforce new regulations curbing the use of virtual private networks (VPN)."

Cybersecurity

25.01.18

Security Brief Asia

[Millions of DDoS attacks hit Asia Pacific in 2017](#)

According to a report by NETSCOUT Arbor, a leading provider of business assurance and cybersecurity, the number of distributed denial of service (DDoS) attacks in Pan-Asia are on the rise.

"Automation and managed services may be the key mechanisms for fighting distributed denial of service (DDoS) attacks, according to new findings from NETSCOUT Arbor."

"The 13th Annual Worldwide Infrastructure Security Report (WISR) confirms the prevalence and scale of DDoS attacks, particularly against service providers and enterprises."

31.01.18

Security Brief Asia

[2017 brought a surge of ransom & hijack attacks against APAC](#)

According to a new report, the Asia Pacific region is becoming a hotbed for ransomware, hijackers, spyware and worms.

"Asia Pacific is a hotspot for ransomware, hijackers, spyware and worms and one security expert believes that the region is becoming a major target – the healthcare and education sectors in particular."

"Malwarebytes' Cybercrime Tactics and Techniques: 2017 State of Malware Report says that across Asia Pacific, the most prevalent threats compared to 2016 were ransomware (1000% increase); hijackers (522% increase); spyware (200% increase); and worms (50% increase)."

Privacy

26.01.18

Cisco

Privacy Maturity Benchmark Study

According to a report by technology company Cisco the most 'privacy-immature' companies have suffered from seventy four percent of cyber losses over £500,000 compared to thirty nine percent of 'mature' companies.

"The General Data Protection Regulation (GDPR) will become fully enforceable on May 25, 2018. Many organizations are rightly investing in resources and processes to meet the GDPR standards and avoid significant fines and other penalties."

"In addition, the many data breaches that exposed the personal information of millions of customers have made organizations increasingly concerned about the products they buy and with whom they partner. Customers are asking more questions during the buying cycle about how data is captured, transferred, stored, and deleted. In this study, Cisco shares insights on how data privacy concerns are impacting the buying cycle."

28.01.18

The Hill

Intel told Chinese firms about chip flaw before US govt: report

According to security experts, the technology firm Intel told the Chinese Government about their security flawed chips before the United States Government, giving Beijing the potential opportunity to exploit them.

"Intel Corporation warned a handful of customers, including several Chinese technology firms, about security flaws within its processor chips before the U.S. government, The Wall Street Journal reported Sunday."

"Security experts told the newspaper that the decision could have allowed Chinese tech companies to flag the vulnerabilities to Beijing, giving the Chinese government an opportunity to exploit them."

31.01.18

The Verge

[China denies claims it built backdoors into African Union's headquarters for spying](#)

French newspaper, Le Monde, has reported that China used the Africa Union's IT division to 'spy' on the nations in the Union. China was the one to finance and build the building and so had access to the system.

"The African Union, a coalition of 55 countries established in Addis Ababa, Ethiopia, has reportedly been a victim of state-sponsored espionage after an investigation from French newspaper Le Monderevealed China was using the computers in a new building's IT division to spy on its continental neighbors.

China was able to do this because it financed and built the new building itself to act as the African Union's new headquarters and gifted it under false pretenses of cordial partnership, Le Monde reports. The spying has reportedly been happening since 2012 when the building opened in downtown Addis Ababa. The backdoor into the African Union's computer systems was first discovered in January 2017, when engineers in the IT division noticed an unusual spike of activity late into the evening when the building was no longer staffed."

Internet Inclusion

30.01.18

Channel NewsAsia

[Google closes HTC deal; Taiwan now largest engineering site in Asia Pacific](#)

Technology company Google is expanding its presence in the Asia- Pacific region after it announced it had secured a deal with Taiwanese Handset Maker HTC. Taiwan will be the largest engineering site for the technology giant.

"Google on Tuesday (Jan 30) announced it has officially closed its deal with Taiwanese handset maker HTC.

"In a blog post by the company's senior vice president for Hardware Rick Osterloh, he said it is welcoming an "incredibly talented team" who have decades of experience "achieving a series of firsts" in the smartphone industry.

These include bringing the first 3G smartphone to market in 2005, the first touch-centric phone in 2007 and the first all-metal unibody phone in 2013, he explained."

Rest of the World

Internet governance

25.01.18

Channel NewsAsia

[Russia's finance ministry ready to regulate, not ban crypto-FX](#)

Following the surge in crypto-currency use, the Finance Ministry in Russia has started working towards regulation for transactions. The Ministry stated no plans to ban the currency but maintained that it would not become a means of payment.

"Russia's finance ministry said on Thursday it was working on legislation that would regulate crypto-currency transactions without fully banning them, although it would not let digital FX be used as a mean of payment in Russia.

The finance ministry said its legislation on crypto-currencies and 'initial coin offerings' envisages allowing such deals only through digital exchanges."

Cybersecurity

26.01.18

SC Media

[Global tech firms let Russian defence agency peek at source code for flaws](#)

American and European tech companies, McAfee, Symantec, Micro Focus and SAP have given the Russian Defence Agency their consent to uncover vulnerabilities in their systems.

"A handful of tech companies have given a Russian defence agency the opportunity to sort the source code of their software, to uncover vulnerabilities that the Russians say could be exploited by bad actors."

"McAfee, Symantec, Micro Focus and SAP all have submitted to the practice, sparking concern at the Pentagon and among lawmakers, according to a Reuters review of both US defence contracts and Russian regulatory requirements."

Privacy

26.01.18

Cisco

[Privacy Maturity Benchmark Study](#)

According to report by technology company Cisco, the most 'privacy-immature, companies suffered from seventy four percent of cyber losses over £500,000 compared to thirty nine percent of 'mature' companies.

"The General Data Protection Regulation (GDPR) will become fully enforceable on May 25, 2018. Many organizations are rightly investing in resources and processes to meet the GDPR standards and avoid significant fines and other penalties."

"In addition, the many data breaches that exposed the personal information of millions of customers have made organizations increasingly concerned about the products they buy and with whom they partner. Customers are asking more questions during the buying cycle about how data is captured, transferred, stored, and deleted. In this study, Cisco shares insights on how data privacy concerns are impacting the buying cycle."

30.01.18

The Guardian Nigeria

[NCC insists on revoking licenses of erring telecoms operators](#)

Penalties are set to be rolled out to telecom operators that mask international telephone calls. The Nigerian Communications Commission hope this will reduce call masking.

"The Nigerian Communications Commission (NCC) has said it would penalise and possibly revoke the licenses of any telecommunication operators implicated in masking international telephone calls. It explained that its recent intervention has resulted in reduced call masking and refilling in the industry.

In spite of the positive development, the commission insisted that the operating licenses of some of the interconnect exchange and other licensees involved in the practice would either be revoked or suspended in the coming weeks."

31.01.18

The Verge

[China denies claims it built backdoors into African Union's headquarters for spying](#)

French newspaper, Le Monde, has reported that China used the Africa Union's IT division to 'spy' on the nations in the Union. China was the one to finance and build the building and so had access to the system.

"The African Union, a coalition of 55 countries established in Addis Ababa, Ethiopia, has reportedly been a victim of state-sponsored espionage after an investigation from French newspaper Le Monderevealed China was using the computers in a new building's IT division to spy on its continental neighbors.

China was able to do this because it financed and built the new building itself to act as the African Union's new headquarters and gifted it under false pretenses of cordial partnership, Le Monde reports. The spying has reportedly been happening since 2012 when the building opened in downtown Addis Ababa. The backdoor into the African Union's computer systems was first discovered in January 2017, when engineers in the IT division noticed an unusual spike of activity late into the evening when the building was no longer staffed."

Internet Inclusion

31.01.18

The Guardian Nigeria

[UK hits 95% broadband penetration as Nigeria struggles at 21%](#)

The UK Government revealed that ninety-five percent of its premises have access to superfast broadband compared to just twenty-one percent in Nigeria. The Nigeria Communications Commission has been accused of not following the National Broadband Plan.

"Though, the Nigerian Communications Commission (NCC), has assured that Nigeria would meet and surpass the 30 per cent penetration target, however, stakeholders are sort of skeptical. They based their argument on the National Broadband Plan (NBP), which is not been followed adequately.

According to them, the NBP is a five-year plan (2013 to 2018), with each year having a particular target, 'but as it is now, we are nowhere near achieving any substantial part of the plan. So, achieving 30 per cent penetration by year end appears bleak.'"

Global Institutions

NATO

[Joint press conference](#)

During a joint press conference, Secretary General for NATO Jens Stoltenberg announced that a new NATO cyber academy was being built in Portugal to discover the next generation of cyber experts.

"Thank you so much. And it's a great honour to be here and to once again meet with you. We have met many many times, but this is actually our first meeting in Lisbon. And for me it is a great honour to be here because Portugal is such a key Ally in our Alliance."

"Portugal makes NATO more secure - on land, at sea, in the air and also in cyber-space. We are very grateful for your many contributions."

Diary Dates

GDPR Summit – 30.01.18

London, England

Manusec Europe – 07.02.18-08.02.18

Munich, Germany

Global Internet and Jurisdiction Conference 2018 – 26.02.18-28.02.18

Ottawa, Canada

Cybersecurity and Data Opportunities in Sub-Saharan Africa – 05.03.18

London, England

Living in the Internet of Things- Cybersecurity of the IoT – 28.03.18-29.03.18

London, England

RSA – 16.04.18–20.04.18

San Francisco, USA

Data Centre Risk Radar- Technical Skills Shortage – 26.04.18

London, England

Africa Internet Summit – 29.04.18-11.05.18

Dakar, Senegal