14 November 2018

Synopsis

Scroll to read full summaries with links to news articles.

Telecom Regulatory Authority of India, **TRAI** have said that they are willing to 'step in' if there is any anti-competitive behaviour between the mobile phone companies. In a statement they said, 'a four-player market is fairly healthy and offers a competitive environment. But if it is anti-competitive or predatory, we'll step in."

The fifth **World Internet Conference** forum was held on November 7-9th in the **Wuzhen**, Zhejiang province. Several topics were discussed including, **FinTech** and Construction of a **Social Credit System**, the Future of Internet, **The Internet of Things**: Towards a Connected World, **AI** and bridging the digital divide.

Telecom Regulatory Authority of India, **TRAI** have asked for expert advice on whether to impose regulations on communication apps such as **WhatsApp**, **Skype** and **Viber** on grounds of national security.

In six months', time, **EU** Member States will be freely sharing non-personal data, including **artificial intelligence** and **machine learning** across the EU, after the European Union Council approved a regulation, to take effect in six months that would make this a reality. The new rules will also ban, "**data localization** restrictions imposed by member states on the geographical location for storing or processing **non-personal data**, unless such restrictions are justified on grounds of public security.'

A new **International Cybersecurity Arrangement** has been signed by more than 50 nations, including the **UK** and 130 groups such as **Microsoft**, **Facebook** and **LinkedIn**. While the agreement is not legally binding, it creates a national standard for **cybersecurity** and cyber warfare, human rights and curbing election manipulation. Among other countries, the **United States**, **Russia** and **China** failed to sign the agreement.

European Union Agency for Network and Information Security (**ENISA**), the European Defence Agency (**EDA**) and the Computer Emergency Response Team for the EU Institutions, Agencies and Bodies (**CERT-EU**) met last week

and agreed to work closer and share more information in regards to **cybersecurity**.

The **United States** congressional advisory panel has advised the country to not purchase internet-linked devices manufactured in **China** because it could potentially leave the US exposed to **security breaches**.

Internet giant **Facebook** has teamed up with **North West-based Agent Academy and The Extraordinary Club**, a company involved in promoting the creative industries, to deliver certified **digital skills training** in the North West of **England** as part of the platform's Community Boost Programme. As part of the programme, Facebook is also partnering with **Freeformers**, a training provider, to offer to upskill 75,000 people across the EU in UK, France, Germany, Poland, Italy and Spain. The training will be for individuals between the ages of 18 and 30 that have little or strong digital skills.

According to the **Digital Rights in Africa** report by Paradigm Initiative, African Governments are passing legislation that harms digital rights and restricts the freedom of expression of citizens. The report mentions eight countries across North, East, West and Central Africa including, Egypt, Morocco, Nigeria and Benin for being the main culprits of this.

The **Chartered Institute of Bankers** in **Nigeria** have announced plans to reorganise the curriculum so banking personnel get more **training** that meets to standards of FinTech's and prepares them for the technology revolution.

According to **Andrew Vogues**, Threat Prevention Sales Leader, Middle East & Africa, at Checkpoint, a leading provider of **cybersecurity** solutions said **Nigeria** needs to take 'cybersecurity challenges seriously' as the attacks continue to rise.

According to **Prof. Paul Theron,** an Advisor to the European Commission and member of NATO's cybersecurity research group claims that 50,000 more cyber experts will be needed to deal with the state-sponsored **cyber espionage** from **Russia**.

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

14 November 2018

Table of Contents

Europe

Internet governance

12.11.18

Computer Weekly

Government considering dedicated internet regulator, says digital minister

According to Margot James, the UK Digital Minister, the Department for Digital, Culture Media and Sport are looking to create a body solely dedicated to regulating the internet because the current system is failing.

"Digital minister Margot James has told the House of Lords Communications Committee that the Department for Digital, Culture, Media and Sport (DCMS) is likely to recommend the creation of some form of dedicated regulatory body for the internet in the next few months."

"Giving evidence to the ongoing Lords inquiry on internet regulation, James said that at the moment, some aspects of online activity were regulated by a number of different bodies, such as telecoms regulator Ofcom, the Advertising Standards Agency (ASA) and the Information Commissioner's Office (ICO), and this approach was no longer viable."

Cybersecurity

03.11.18

The Telegraph

Britain needs a 50,000-strong cyber army to protect against prolific Russian hackers, warns Nato adviser

According to Prof Paul Theron**,** an Advisor to the European Commission and member of NATO's cybersecurity research group claims that 50,000 more cyber experts will be needed to deal with the state-sponsored cyber espionage from Russia.

"Britain will be wide-open to state-sponsored hacking of its critical infrastructure - including its energy supply - for the next decade because of a shortage of 50,000 cyber-security specialists, a top Nato adviser has warned."

"Prof Paul Theron, a member of Nato's cyber-security research group and an advisor to the European Commission, said Britain urgently needed to bolster its defences against what he called a now "constant" barrage of sophisticated attacks from state-sponsored and criminal organisations against power stations, electricity networks and other essential systems."

08.11.18

Europol

EU cybersecurity organisations agree on 2019 roadmap

European Union Agency for Network and Information Security (ENISA), the European Defence Agency (EDA) and the Computer Emergency Response Team for the EU Institutions, Agencies and Bodies (CERT-EU) met last week and agreed to work closer and share more information in regards to cybersecurity.

"On 6 November 2018, following a meeting at working level, the four Principals of the Memorandum of Understanding (MoU) between Europol, the European Union Agency for Network and Information Security (ENISA), the European Defence Agency (EDA), and the Computer Emergency Response Team for the EU Institutions, Agencies and Bodies (CERT-EU), met at CERT-EU's premises."

"The purpose of the meeting was to update each other on relevant developments and assess the progress made under the MoU, which provides a cooperation framework aiming at leveraging synergies between the four organisations to achieve a safe and open cyberspace."

14.11.18

IT Pro Portal

UK and 50 nations sign cyber security pact

A new International Cybersecurity Arrangement has been signed by more than 50 nations, including the UK and 130 groups such as Microsoft, Facebook and LinkedIn. While the agreement is not legally binding, it creates a national standard for cybersecurity and cyber warfare, human rights and curbing election manipulation. Among other countries, the United States, Russia and China failed to sign the agreement.

"The UK, together with more than 50 nations, has signed an international cybersecurity agreement that aims to put some standards on cyber security and cyber warfare. The agreement was released by the French president Emmanuel Macron, during the Paris Peace Forum."

"Fifty nations aside, the agreement was also signed by 130 groups from the private sector, as well as 90 charitable groups and universities. Cybersecurity Tech Accord, which includes companies like Microsoft, Facebook, LinkedIn, Oracle and Salesforce, also signed."

14.11.18

EIOPA

Joint Statement: EU and U.S. insurance regulators continue the dialogue on cyber security, cyber insurance, the use of big data and intra-group transactions

During the recent EU – US forum, the European Insurance and Occupational Pensions Authority (EIOPA), the National Association of Insurance Commissioners (NAIC) and the Federal Insurance Office (FIO) of the U.S. Department of Treasury, regulators from the US and the EU shared multiple perspectives on the challenges and opportunities posed by cyber risks and AI.

"Growing cyber threats, increasing power of big data as well as contagion risk from intra-group transactions in multi-national insurance groups are focus areas for risk-based and forward-looking supervision in the United States and the European Union."

"The Steering Committee of the EU -U.S. Insurance Dialogue Project set the scene for 2019 for further deepening the cooperation and mutual understanding of regulatory approaches and supervisory practices in these evolving and critical areas."

Privacy

12.11.18

Computer Weekly

EU regulation set to advance single market for non-personal data

In six months', time, EU Member States will be freely sharing non-personal data, including artificial intelligence and machine learning across the EU, after the European Union Council approved a regulation, to take effect in six months that would make this a reality. The new rules will also ban, "data localization restrictions imposed by member states on the geographical location for storing or processing non-personal data, unless such restrictions are justified on grounds of public security.'

"The European Union Council and Parliament have approved a regulation, to take effect in six months' time, to ensure the free movement of non-personal data, such as IoT data, across the bloc."

"The European Union Council, made up of the heads of government of member states, has rubber-stamped a set of new rules to bring down barriers to the free movement of non-personal data across the EU."

Internet Inclusion

07.11.18

Council of Europe

Council of Europe to take part in Internet Governance Forum in Paris

The thirteenth Annual Meeting of the Internet Governance Forum took place at UNESCO headquarters in Paris from the 12th to 14th November, under the heading of "Internet of Trust.' The forum brought together representatives of Government, the technology sector and businesses to discuss disinformation, data protection, privacy and artificial intelligence.

"A Council of Europe delegation will take part in discussions to be held at the Internet Governance Forum (IGF) at UNESCO headquarters in Paris from 12 to 14 November, under the heading of 'Internet of Trust'."

"Throughout the Forum, which will bring together representatives of governments, international organisations, businesses, civil society, academia and the technological sector, the Council of Europe will contribute to the debates on defending human rights and democracy online. The topics to be discussed will include disinformation, artificial intelligence, children's rights, data protection, the right to privacy and hate speech."

08.11.18

London Business

Facebook selects first UK digital skills training partner

Internet giant Facebook has teamed up with North West-based Agent Academy and The Extraordinary Club, a company involved in promoting the creative industries, to deliver certified digital skills training in the North West of England as part of the platform's Community Boost Programme. As part of the programme, Facebook is also partnering with Freeformers, a training provider, to offer to upskill 75,000 people across the EU in UK, France, Germany, Poland,

Italy and Spain. The training will be for individuals between the ages of 18 and 30 that have little or strong digital skills.

"North West-based Agent Academy and The Extraordinary Club have been selected by Freeformers and Facebook to deliver certified digital skills training in the North West of England as part of the platform's Community Boost programme, which aims to equip more people in Europe with the digital skills they need to compete in today's workplace."

"The training focuses on enabling people to develop confidence and skills for future employment in a digital economy – especially those found to be lacking in the current workforce – with students at The City of Liverpool College being the first cohort to take part."

09.11.18

Public Technology

Government trials 'learn to code' tool for civil servants

The UK Civil Service have created a new online tool with the aim of teaching their Government employees how to code. Six different modules are being offered including how to build webpages and databases.

"A group of people on the Civil Service Fast Stream development programme have built an online tool to teach their fellow government employees to code."

"The Learn to code site – which is currently in open beta phase – has been constructed as a step-by-step service, and currently covers six different modules: getting started; learning how the web works; building webpages; adding interactivity; web services; and databases."

United States of America

Internet governance

No new items of relevance

Cybersecurity

04.11.18

The Hill

Scott Walker puts Wisconsin National Guard cyber team on standby for Election Day

Scott Walker, the Governor of Wisconsin said that during the midterm elections the National Guard's cybersecurity team were on standby to help in case of any cyber concerns. However, election officials have not yet seen any sign of interference.

"Wisconsin Gov. Scott Walker (R) on Friday activated his state National Guard's cybersecurity teams to be on standby for Tuesday's midterms."

"Wisconsin voters should feel confident that the Wisconsin National Guard's team is ready if needed to provide assistance on Election Day," said Maj. Gen. Donald Dunbar in the National Guard's announcement of the move."

13.11.18

The Hill

Russia pushes for court to throw out DNC lawsuit

The Democratic National Committee is suing the Russian Government for their alleged interference in the 2016 election. The Russian Government is seeking to dismiss this lawsuit and has warned that if the lawsuit proceeds, other spy services in the US 'could be exposed to litigation In response.'

"The Russian government is seeking the dismissal of a lawsuit brought by the Democratic National Committee (DNC) related to alleged interference in the 2016 election."

"The Washington Post reported that the Russian Ministry of Justice penned a letter last week to the State Department and a judge in New York's Southern District arguing that the lawsuit violates the United States' Foreign Sovereign Immunities Act."

14.11.18

EIOPA

Joint Statement: EU and U.S. insurance regulators continue the dialogue on cyber security, cyber insurance, the use of big data and intra-group transactions

During the recent EU – US forum, the European Insurance and Occupational Pensions Authority (EIOPA), the National Association of Insurance Commissioners (NAIC) and the Federal Insurance Office (FIO) of the U.S. Department of Treasury, regulators from the US and the EU shared multiple perspectives on the challenges and opportunities posed by cyber risks and AI.

"Growing cyber threats, increasing power of big data as well as contagion risk from intra-group transactions in multi-national insurance groups are focus areas for risk-based and forward-looking supervision in the United States and the European Union."

"The Steering Committee of the EU -U.S. Insurance Dialogue Project set the scene for 2019 for further deepening the cooperation and mutual understanding of regulatory approaches and supervisory practices in these evolving and critical areas."

14.11.18

IT Pro Portal

UK and 50 nations sign cyber security pact

A new International Cybersecurity Arrangement has been signed by more than 50 nations, including the UK and 130 groups such as Microsoft, Facebook and LinkedIn. While the agreement is not legally binding, it creates a national standard for cybersecurity and cyber warfare, human rights and curbing election manipulation. Among other countries, the United States, Russia and China failed to sign the agreement.

"The UK, together with more than 50 nations, has signed an international cybersecurity agreement that aims to put some standards on cyber security and cyber warfare. The agreement was released by the French president Emmanuel Macron, during the Paris Peace Forum."

“Fifty nations aside, the agreement was also signed by 130 groups from the private sector, as well as 90 charitable groups and universities. Cybersecurity Tech Accord, which includes companies like Microsoft, Facebook, LinkedIn, Oracle and Salesforce, also signed.”

Privacy

31.10.18

Nextgov

Dems question if Google violated FTC privacy settlement

The United States are investigating whether internet giant Google has by failing to disclose a software vulnerability that effected the data of more than half a million Google Plus users, violated a consent agreement with the Federal Trade Commission.

“Two Democratic senators are questioning if Google violated a consent agreement with the Federal Trade Commission (FTC) in failing to disclose a software vulnerability that exposed the data of nearly half a million Google Plus users.”

“Sens. Catherine Cortez Masto (Nev.) and Amy Klobuchar (Minn.) on Wednesday sent a letter to Google CEO Sundar Pichai expressing their concerns about the exposure and the company’s response to it.”

14.11.18

ABC News

US panel warns against government purchase of Chinese tech

The United States congressional advisory panel has advised the country to not purchase internet-linked devices manufactured in China because it could potentially leave the US exposed to security breaches.

“A congressional advisory panel says the purchase of internet-linked devices manufactured in China leaves the United States vulnerable to security breaches that could put critical infrastructure at risk.”

“In its annual report on Wednesday, the U.S.-China Economic and Security Review Commission warns of dangers to the U.S. government and private sector from a reliance on global supply chains linked to China, which is the world's largest manufacturer of information technology equipment.”

Internet Inclusion

08.11.18

London Business

Facebook selects first UK digital skills training partner

Internet giant Facebook has teamed up with North West-based Agent Academy and The Extraordinary Club, a company involved in promoting the creative industries, to deliver certified digital skills training in the North West of England as part of the platform's Community Boost Programme. As part of the programme, Facebook is also partnering with Freeformers, a training provider, to offer to upskill 75,000 people across the EU in UK, France, Germany, Poland, Italy and Spain. The training will be for individuals between the ages of 18 and 30 that have little or strong digital skills.

"North West-based Agent Academy and The Extraordinary Club have been selected by Freeformers and Facebook to deliver certified digital skills training in the North West of England as part of the platform's Community Boost programme, which aims to equip more people in Europe with the digital skills they need to compete in today's workplace."

"The training focuses on enabling people to develop confidence and skills for future employment in a digital economy – especially those found to be lacking in the current workforce – with students at The City of Liverpool College being the first cohort to take part."

15.11.18

Nextgov

LinkedIn CEO Jeff Weiner Says the Biggest Skills Gap In the U.S. Is Not Coding

Chief Executive of LinkedIn, Jeff Weiner, has said the biggest skills gap in the US is for soft skills such as written communication, oral communication and leadership skills, instead of coding, which is what is commonly thought.

"Ask anyone which professional skill is most in demand right now, and they'll likely say coding. But ask LinkedIn CEO Jeff Weiner, and he'll give you a different answer."

"As head of the world's largest professional-networking site, Weiner presumably has access to more, and more detailed, employment information than any government. He knows what jobs people post, what jobs people have, and what jobs people want. And the biggest skills gap he says he sees in the United States is soft skills."

Pan-Asia

Internet governance

13.11.18

Gadgets Now

TRAI seeks views on regulating messaging apps like WhatsApp, Skype

Telecom Regulatory Authority of India, TRAI have asked for expert advice on whether to impose regulations on communication apps such as WhatsApp, Skype and Viber on grounds of national security.

"The telecom regulator has sought views on whether communications apps such as WhatsApp, Skype and Viber should be regulated, mainly in light of economic and security matters, a move that these services and backers of net neutrality have opposed."

"In a paper released Monday, the Telecom Regulatory Authority of India invited industry's views to identify which of these apps should be regarded as providing the same services as mobile phone operators. It also wanted to look into the costs and benefits of bringing these communication apps – known as over-the-top (OTT) services – under the regulatory regime."

14.11.18

Gadgets Now

TRAI chief warns telecom companies against cartelisation

Telecom Regulatory Authority of India, TRAI have said that they are willing to 'step in' if there is any anti-competitive behaviour between the mobile phone companies. In a statement they said, 'a four-player market is fairly healthy and offers a competitive environment. But if it is anti-competitive or predatory, we'll step in."

"New Delhi: The Telecom Regulatory Authority of India (Trai) has cautioned mobile phone companies against any anti-competitive behaviour, saying the sectoral watchdog will step in if there is any hint of cartelization in an industry reduced to three private players, plus one state-run telco."

"A four-player market is fairly healthy and offers a competitive environment. But if it is anti-competitive or predatory, we'll step In", Telecom Regulatory Authority of

India (Trai) chairman Ram Sewak Sharma told ET in an interview."

14.11.18

Gadgets Now

Data localisation is not protectionist approach: FICCI president

According to Rashesh Shah, the President of the Federation of Indian Chambers of Commerce and Industry said, 'data localisation is not protectionist, it's to manage local interests.'

"India's push for data localisation is not a "protectionist" approach but it is to "manage" local interests, head of a top Indian industry body said her on Tuesday."

"Data localisation requires data about residents be collected, processed, and stored inside the country, often before being transferred internationally and usually transferred only after meeting local privacy or data protection laws."

Cybersecurity

14.11.18

IT Pro Portal

UK and 50 nations sign cyber security pact

A new International Cybersecurity Arrangement has been signed by more than 50 nations, including the UK and 130 groups such as Microsoft, Facebook and LinkedIn. While the agreement is not legally binding, it creates a national standard for cybersecurity and cyber warfare, human rights and curbing election manipulation. Among other countries, the United States, Russia and China failed to sign the agreement.

"The UK, together with more than 50 nations, has signed an international cybersecurity agreement that aims to put some standards on cyber security and cyber warfare. The agreement was released by the French president Emmanuel Macron, during the Paris Peace Forum."

"Fifty nations aside, the agreement was also signed by 130 groups from the private sector, as well as 90 charitable groups and universities. Cybersecurity Tech Accord, which includes companies like Microsoft, Facebook, LinkedIn, Oracle and Salesforce, also signed."

Privacy

14.11.18

ABC News

US panel warns against government purchase of Chinese tech

The United States congressional advisory panel has advised the country to not purchase internet-linked devices manufactured in China because it could potentially leave the US exposed to security breaches.

"A congressional advisory panel says the purchase of internet-linked devices manufactured in China leaves the United States vulnerable to security breaches that could put critical infrastructure at risk."

"In its annual report on Wednesday, the U.S.-China Economic and Security Review Commission warns of dangers to the U.S. government and private sector from a reliance on global supply chains linked to China, which is the world's largest manufacturer of information technology equipment."

Internet Inclusion

06.11.18

ChinaDaily

Colleges, firms tackle talent shortages

Chinese Universities are doing more to tackle the digital skills gap by combining practical experience of online attacks with cybersecurity theories to help graduates gain the skills in demand by industries.

"Efforts ramped up to bridge the gap of cybersecurity sector's needs."

"Chinese university courses are starting to combine practical experience of online attacks with cybersecurity theories, with help and oversight from security enterprises, in a move to effectively meet the industry's demand for talented graduates."

08.11.18

ChinaDaily

Chinese carriers wrest 5G lead

The fifth World Internet Conference forum was held on November 7-9th in the Wuzhen, Zhejiang province. Several topics were discussed including, FinTech and Construction of a Social Credit System, the Future of the Internet, AI and bridging the digital divide.

"Intensified research and development activities, industry partnerships mark the push toward 2020 commercial rollout."

"Editor's Note: On Friday, the ongoing Fifth World Internet Conference in Wuzhen, Zhejiang province, will hold a forum on "5G Era: Opening and Cooperation for a Better Future". In the run-up to the key event, in interviews with China Daily, industry luminaries recalled how China's sustained R&D efforts have helped the nation maintain its pioneering role in evolving 5G mobile communication technology, related standards and the licensing phase."

Rest of the World

Internet governance

No new items of relevance

Cybersecurity

03.11.18

The Telegraph

Britain needs a 50,000-strong cyber army to protect against prolific Russian hackers, warns Nato adviser

According to Prof Paul Theron**,** an Advisor to the European Commission and member of NATO's cybersecurity research group claims that 50,000 more cyber experts will be needed to deal with the state-sponsored cyber espionage from Russia.

"Britain will be wide-open to state-sponsored hacking of its critical infrastructure - including its energy supply - for the next decade because of a shortage of 50,000 cyber-security specialists, a top Nato adviser has warned."

"Prof Paul Theron, a member of Nato's cyber-security research group and an advisor to the European Commission, said Britain urgently needed to bolster its defences against what he called a now "constant" barrage of sophisticated attacks from state-sponsored and criminal organisations against power stations, electricity networks and other essential systems."

13.11.18

The Hill

Russia pushes for court to throw out DNC lawsuit

The Democratic National Committee is suing the Russian Government for their alleged interference in the 2016 election. The Russian Government is seeking to dismiss this lawsuit and has warned that if the lawsuit proceeds, other spy services in the US 'could be exposed to litigation In response.'

"The Russian government is seeking the dismissal of a lawsuit brought by the Democratic National Committee (DNC) related to alleged interference in the 2016 election."

"The Washington Post reported that the Russian Ministry of Justice penned a letter last week to the State Department and a judge in New York's Southern District arguing that the lawsuit violates the United States' Foreign Sovereign Immunities Act."

14.11.18

The Guardian

'Nigeria should take cyber security challenges seriously'

According to Andrew Vogues, Threat Prevention Sales Leader, Middle East & Africa, at CheckPoint, a leading provider of cybersecurity solutions said Nigeria needs to take 'cybersecurity challenges seriously' as the attacks continue to rise.

"Andrew Vogues is the Threat Prevention Sales Leader, Middle East & Africa, CheckPoint, a multinational provider of software and combined hardware and software products for IT security. He spoke with OLUWATOSIN AREO, on the need for adequate cyber security prevention in the country."

"Cyber security is on the up-rise and it has been for the last few years. What we focus on at Checkpoint is prevention particularly from cyber security perspective. Traditional security was only at the perimeter."

14.11.18

IT Pro Portal

UK and 50 nations sign cyber security pact

A new International Cybersecurity Arrangement has been signed by more than 50 nations, including the UK and 130 groups such as Microsoft, Facebook and LinkedIn. While the agreement is not legally binding, it creates a national standard for cybersecurity and cyber warfare, human rights and curbing election manipulation. Among other countries, the United States, Russia and China failed to sign the agreement.

"The UK, together with more than 50 nations, has signed an international cybersecurity agreement that aims to put some standards on cyber security and cyber warfare. The agreement was released by the French president Emmanuel Macron, during the Paris Peace Forum."

"Fifty nations aside, the agreement was also signed by 130 groups from the private sector, as well as 90 charitable groups and universities. Cybersecurity

Tech Accord, which includes companies like Microsoft, Facebook, LinkedIn, Oracle and Salesforce, also signed."

Privacy

No new items of relevance

Internet Inclusion

03.11.18

IT News Africa

Mastercard announces new fund to Seed young African leaders

Mastercard Foundation, which seeks to improve the education and training of young people across 29 countries in Africa has announced a new fund to help young people kick-start their careers.

"Mastercard Foundation today announced a new fund that will enable young changemakers to seed and kick-start promising social ventures and community projects, creating economic opportunities for themselves and others."

"Over the next two years, the Foundation will dedicate US$2M for a pilot project that will expand Mastercard Foundation Scholars' capacity to exercise transformative leadership by putting their social and entrepreneurial ideas into action."

14.11.18

The Guardian

How African governments use repressive laws in the digital age

According to the Digital Rights in Africa report by Paradigm Initiative, African Governments are passing legislation that harms digital rights and restricts the freedom of expression of citizens. The report mentions countries across North, East, West and Central Africa including, Egypt, Morocco, Nigeria and Benin for being the main culprits of this.

"We live in a fast-changing world, and the digital rights and media freedom landscape are not immune to that."

“There are many examples of this incidence, but perhaps none is as evident as the rising tide of nations claiming national sovereignty over the internet.”

14.11.18

The Guardian

CIBN rejigs curriculum to enhance fintechs operations

The Chartered Institute of Bankers in Nigeria have announced plans to reorganise the curriculum so banking peronsell get more training that meets the standards of FinTech’s and prepares them for the technology revolution.

“The Chartered Institute of Bankers in Nigeria (CIBN), has rejigged its curriculum to accommodate more aspects of Fintechs and enhance better financial service delivery.”

“The Institute during the Fintech Association of Nigeria (FintechNGR) Social Meet 3.0, in Lagos, harped on the need for regular training of banking personnel to meet up with the technology revolution.”

Global Institutions

03.11.18

The Telegraph

Britain needs a 50,000-strong cyber army to protect against prolific Russian hackers, warns Nato adviser

According to Prof Paul Theron**,** an Advisor to the European Commission and member of NATO's cybersecurity research group claims that 50,000 more cyber experts will be needed to deal with the state-sponsored cyber espionage from Russia.

"Britain will be wide-open to state-sponsored hacking of its critical infrastructure - including its energy supply - for the next decade because of a shortage of 50,000 cyber-security specialists, a top Nato adviser has warned."

"Prof Paul Theron, a member of Nato's cyber-security research group and an advisor to the European Commission, said Britain urgently needed to bolster its defences against what he called a now "constant" barrage of sophisticated attacks from state-sponsored and criminal organisations against power stations, electricity networks and other essential systems."

Diary Dates

Cyber Security Industry Roundtable - Brazil – 27.11.19

London, England

Women in Defence Technology – 12.02.19

London England

Mobile World Congress – 25.02.19

London England