



**04 April 2018**

## Synopsis

**Scroll to read full summaries with links to news articles.**

An **Anti-Fake News Bill** has passed the policy stage in the **Dewan Rakyat**, the lower house of the Parliament of **Malaysia**. The Bill seeks to stop the spread of fake news by threatening those who spread fake news with six years in prison.

According to Software company, **Symantec**, **cybersecurity** threats have worsened in **Thailand** in 2017 compared to 2016, as more devices were connected and the country took more interest in **cryptocurrency** and exchanges.

**Thailand** and **Japan** are partnering to create a ASEAN-Japan **Cybersecurity** Capacity Building Centre in Thailand in June this year. 700 cybersecurity personnel will be trained to fight cybercrime in the region.

The **United States** have passed the **Cloud Act** which gives law enforcement and Governments around the world, including **Britain**, unprecedented powers to access and use private online information including emails, documents, credit card transactions and photos to prosecute citizens.

The European Commissioner for security, **Sir Julian King** said **social media** companies need to be governed during campaign periods and a 'clear game plan' needs to be established to limit the spread of **fake news** online.

According to a **privacy rights** charity, 26 forces including **Police** Scotland are using **espionage technology** to extract photos, passwords and emails of witnesses, suspects and victims without a warrant or permission from those they are searching.

Internet giant **Facebook** have announced that 87 million user's **personal information** was shared with software company **Cambridge Analytica**, who illegally used this data to influence the **United States** elections.

The **United States** Government have given states a \$380 million fund to ensure their **voting technology** is protected and secure from **cyber threats**.

**Apple** has announced that it will stop using **Intel Chips** in **Mac** computers and will replace them with own, pushing technology company Intel's shares down by 6.1%.

**Privacy advocacy** groups in **Africa** have raised concerns for the limited consensus on **data protection** rules across the continent, warning that this is potentially putting Africa's ever increasing number of internet users at risk.

**Australia** have announced that they will investigate **Facebook** to assess whether the internet giant has breached the countries **privacy laws** by allowing 300,000 Australian users data to be used without permission.

According to the President of the **Institute of Software Practitioners of Nigeria (ISPON)** stakeholders will attend an event on April 6 in Lagos to discuss **Nigeria's** fourth industrial revolution and how the country can harness technology.

The **Internet Telecommunication Union** have published several documents to help support ITU member states to promote economic growth and job creation through **digital innovation**.

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**

04 April 2018

**Table of Contents**

<b>Synopsis</b> .....	<b>1</b>
<b>Europe</b> .....	<b>4</b>
Internet governance.....	4
Cybersecurity .....	5
Privacy.....	5
Internet Inclusion .....	6
<b>United States of America</b> .....	<b>9</b>
Internet governance.....	9
Cybersecurity .....	10
Privacy.....	11
Internet Inclusion .....	14
<b>Pan-Asia</b> .....	<b>15</b>
Internet governance.....	15
Cybersecurity .....	16
Privacy.....	18
Internet Inclusion .....	18
<b>Rest of the World</b> .....	<b>20</b>
Internet governance.....	20
Cybersecurity .....	21
Privacy.....	22
Internet Inclusion .....	23
<b>Global Institutions</b> .....	<b>25</b>
<b>Diary Dates</b> .....	<b>26</b>

## Europe

### Internet governance

**03.04.18**

**The Times**

#### [Brussels to demand curbs on social media during elections](#)

The European Commissioner for security, Sir Julian King said there needs to be a 'clear game plan' for how social media companies are governed during election campaign periods, to limit the spread of fake news online.

*"The EU is to set out measures to curb the spread of disinformation online ahead of next year's elections."*

*"Sir Julian King, the European commissioner for security, has demanded a "clear game plan" to govern how social media companies are allowed to operate during election campaign periods."*

**04.04.18**

**Financial Times**

#### [What the EU's tough new privacy rules mean for Big Tech](#)

The European Union's tough privacy rules come into effect in two months which will mean companies that collect personal information like social media network Facebook will have to gain clear consent and inform users what they do with their personal data.

*"The Facebook-Cambridge Analytica revelations, which have swept the world's largest social network into a weeks-long privacy scandal, have been a test case for data protection rules."*

*"The alleged breach allowed a little-known data analytics company."*

## Cybersecurity

05.04.18

Parliament.uk

### [UK Government needs a long-term Commonwealth strategy, says Committee](#)

The Foreign Affairs Committee has urged the Foreign and Commonwealth Office to consider a new forum to facilitate cross-Commonwealth dialogue around human rights, the rule of law and critical issues such as cyber security, data protection and online privacy.

*“The Foreign Affairs Committee publishes a report, Global Britain and the 2018 Commonwealth Summit, seeking clarity from Government about its long-term vision for the UK’s relationship with the Commonwealth.”*

*“For the first time in more than 20 years, the UK will host the biennial gathering of the Commonwealth Heads of Government. The Commonwealth Summit, a once-in-a-generation event, takes place in London between 16 and 20 April, 2018.”*

## Privacy

01.04.18

The Times

### [Facebook is not only threat to our privacy](#)

The United States have passed the Cloud Act which gives law enforcement and Governments around the world, including Britain, unprecedented powers to access and use private online information including emails, documents, credit card transactions and photos to prosecute citizens.

*“Amid the uproar over the Facebook data-harvesting scandal, something far more significant happened. A large chunk of your digital rights were watered down. On March 23, the US Congress passed a gargantuan spending bill that was stuffed with funding for everything from roads to public parks and drug addiction programmes. Tucked away on page 2,201, however, was a little-noticed addition.”*

*“It was called the Cloud Act — short for the Clarifying Lawful Overseas Use of Data Act. The legislation granted sweeping new powers to law enforcement and governments around the world, including Britain, to harvest and use for prosecution the private online information of their citizens.”*

**02.04.18**

**The Times**

**[Privacy fears as Scottish police use spy tools to break into mobile phones](#)**

According to a privacy rights charity, 26 forces including Police Scotland are using espionage technology to extract photos, passwords and emails of witnesses, suspects and victims without a warrant or permission from those they are searching.

*“Police forces across Britain are using espionage technology to download the entire contents of mobile phones belonging to suspects, witnesses and victims.”*

*“At least 26 forces, including Police Scotland, use the laptop-size devices to extract emails, photos, passwords and conversations on encrypted messaging apps without using a password or thumbprint. According to Privacy International, a privacy rights charity, forces do not obtain warrants or seek permission from the people whose phones they search.”*

**03.04.18**

**The Times**

**[Ireland ‘must follow EU’s lead against fake news to save democracy’](#)**

Ireland has been urged to follow in Brussels steps to crack down on social media companies during election campaigns to stop the spread of fake news.

*“The government has been told that tackling online data regulation is “beyond urgent” as Brussels plans to crack down on social media companies used to spread fake news during elections.”*

*“Sir Julian King, the European security commissioner, said that states faced a threat that could “subvert our democratic systems”. He wants a “clear game plan” to tackle fake news and the use of personal data for political purposes.”*

## **Internet Inclusion**

**28.03.18**

**Migration Advisory Committee**

**[EEA-workers in the UK labour market: Interim Update](#)**

Responding to the Migration Advisory Committee’s inquiry into European migration, industry body TechUK has said that the UK suffers from a digital skills

shortage and highlighted the importance of EU nationals in filling this gap, including after Brexit.

*“In July 2017, the Home Secretary commissioned the MAC to report on the current and likely future patterns of EEA migration and the impacts of that migration on the UK. The intention is to provide an evidence base for the design of a new migration system after the end of the implementation period in 2021.*

*“We were asked to deliver a final report in September 2018, but with an option to produce interim reports.”*

**28.03.18**

### **Computer Weekly**

#### **UK organisations urged to develop cyber security skills**

A new survey by cloud computing firm Rackspace has discovered that the UK is lagging behind other Western nations when it comes to upskilling IT professionals in cybersecurity. IT leaders in the UK set aside a mere 10% of their annual budget to train new hires compared to Germany and the US (14%).

*“Managed cloud computing firm Rackspace is calling on UK organisations to do more to develop cyber security skills in the light of research into expertise in cloud security.”*

*“Failure to develop cyber security skills is exposing organisations to cyber-attacks and exacerbating the skills gap, according to research into the levels of expertise in cloud security and data protection.”*

**28.03.18**

### **Computer Weekly**

#### **Why does India have a higher percentage of women in tech than the UK?**

The Open University has discovered that there is a higher percentage of women in technology roles in India than in the UK. 35% of people with specialists' technology roles in India are women, compared to 17% in the UK.

*“Research by the Open University has assessed the differences between the women in IT landscape in the UK and India.”*

*“The number of women in specialist IT roles in India is significantly higher than in the UK, research by Open University has found.”*

**04.04.18**

**Financial Times**

**[Threat to fintech industry as young coders shun London over Brexit](#)**

Several British technology companies such as global platform payment company, Currencycloud are moving their operations abroad over concerns that Brexit will cause a shortage in skilled workers and hamper growth.

*“British financial technology companies are worried that Brexit is causing a shortage of software engineers and pushing up salaries in the sector, prompting some of them to open offices elsewhere in the EU.”*

*“Mike Lavern, chief executive of Currencycloud, said that the UK-based payments company was planning to open an office in another EU city – probably Amsterdam – because of fears that recruitment problems in London could hamper its growth.”*



## United States of America

### Internet governance

**30.03.18**

**The Hill**

#### [Government doles out election security funds to states](#)

The United States Government have given states a \$380 million fund to ensure their voting technology is protected and secure from cyber threats.

*“The Trump administration has given states \$380 million to upgrade and secure their voting technology.”*

*“The funding was included in the massive appropriations bill approved by Congress and signed by President Trump last week. It represents an effort by lawmakers in Washington to protect upcoming elections from cyber threats, following Russian interference in the 2016 presidential election.”*

**04.04.18**

**Financial Times**

#### [What the EU's tough new privacy rules mean for Big Tech](#)

The European Union's tough privacy rules come into effect in two months which will mean companies that collect personal information like social media network Facebook will have to gain clear consent and inform users what they do with this data.

*“The Facebook-Cambridge Analytica revelations, which have swept the world's largest social network into a weeks-long privacy scandal, have been a test case for data protection rules.”*

*“The alleged breach allowed a little-known data analytics company.”*

## Cybersecurity

**29.03.18**

### **Security Brief Asia**

#### [Businesses are more aware of cybercrime but still not prepared](#)

A new study of 202 senior level security executives in the UK and the US indicates that more cybersecurity awareness does not necessarily lead to businesses putting better safeguards in place. The study found that less than 45% had the technology in place to prevent attacks and only 47% said they had the budget.

*“New research has emerged that reveals better cybersecurity awareness doesn’t necessarily mean better preparation.”*

*“Commissioned by SolarWinds MSP and undertaken by the Ponemon Institute, the study asked 202 senior-level security executives in the US and the UK about emerging security threats.”*

**30.03.18**

### **The Hill**

#### [NYC to launch free cybersecurity tools for residents](#)

New York City have commissioned two free cybersecurity tools to keep the city safe from cyber-attacks. These include a smartphone app which alerts users if their phone has been hacked and a tool known as Quad9 which blocks dangerous sites.

*“New York City will boost its residents’ internet security by rolling out two free cybersecurity tools, New York Mayor Bill de Blasio announced Thursday.”*

*“The NYC Secure program will cost the city about \$5 million per year as it works to protect New Yorkers from facing malicious cyber activity online.”*

**04.04.18**

### **The Hill**

#### [Chinese cyber spies pose challenge for Trump admin](#)

The Trump administration is struggling to deal with Chinese cyber spies that continuously hack into US businesses and steal information from defence contractors.

*“Chinese espionage activity is posing a challenge for the Trump administration as it seeks to crack down on China for allegedly unfair trade practices, including persistent cyber intrusions targeting U.S. businesses.”*

*“While China has largely stopped hacking into U.S. companies to steal intellectual property in accordance with a 2015 Obama-era pact, security experts say Beijing’s spies have continued to break into U.S. networks to advance China’s economic and national security ambitions—testing the limits of the deal.”*

## Privacy

**01.04.18**

**The Times**

### [Facebook is not only threat to our privacy](#)

The United States have passed the Cloud Act which gives law enforcement and Governments around the world, including Britain, the powers to access and use private online information including emails, documents, credit card transactions and photos to prosecute citizens.

*“Amid the uproar over the Facebook data-harvesting scandal, something far more significant happened. A large chunk of your digital rights were watered down. On March 23, the US Congress passed a gargantuan spending bill that was stuffed with funding for everything from roads to public parks and drug addiction programmes. Tucked away on page 2,201, however, was a little-noticed addition.”*

*“It was called the Cloud Act — short for the Clarifying Lawful Overseas Use of Data Act. The legislation granted sweeping new powers to law enforcement and governments around the world, including Britain, to harvest and use for prosecution the private online information of their citizens.”*

**02.04.18**

**The Hill**

### [Civil liberties groups push tech companies to adopt 'security pledge'](#)

Top civil liberties groups, the American Civil Liberties Union and Fight for the Future and Colour of Change have urged technology companies such as Facebook to sign a pledge to commit to protecting their user’s data.

*“Top civil liberties groups and privacy advocates are pressing technology companies to do more to protect their users after Cambridge Analytica*

*improperly collected data from tens of millions of Facebook accounts without users' consent."*

*"The American Civil Liberties Union, Fight for the Future and Color of Change are calling on technology companies to sign a pledge committing them to "to protecting their users' data from exploitation and securing their users' human rights, ensuring their products and services do not put human rights at risk."*

**03.04.18**

**The Times**

**[Apple 'to drop Intel chips'](#)**

Apple has announced that it will stop using Intel Chips in Mac computers following security flaws and will replace them with their own, pushing technology company Intel's shares down by 6.1%.

*"Apple plans to stop using Intel chips in Mac computers in favour of its own ones, Bloomberg reported, pushing shares in the chipmaker down 6.1 per cent."*

*"Apple uses chips and processors from a number of companies, including Qualcomm, Broadcom, Arm and Intel. Intel, which gets about 5 per cent of its revenue from the company, has been supplying chips to Apple since 2005."*

**03.04.18**

**Channel NewsAsia**

**[Indonesia warns Facebook of shutdown if privacy breached: Report](#)**

Rudiantara Indonesia's Communications and Information Minister said if evidence emerges that internet giant Facebook has not adequately protected their citizens data and failed to tackle fake news in the upcoming election then he will shut them down.

*"Indonesia's communications and information minister Rudiantara has threatened to shut down Facebook in the country if there is evidence of citizens' personal data being harvested or if it fails to tackle fake news in the upcoming elections, Bloomberg reported on Tuesday (Apr 3)."*

*"In an interview with the agency, Mr Rudiantara said: "If I have to shut them down, then I will do it.""*

**03.03.18**

**The Hill**

**[US acknowledges potential unauthorized spying devices in DC](#)**

In a letter to United States Senator, Ron Wyden, the Department of Homeland Security said that foreign actors had planted spying devices to track mobile phone activity in Washington DC.

*“The Department of Homeland Security (DHS) is acknowledging for the first time that foreign actors or criminals are using eavesdropping devices to track cellphone activity in Washington, D.C., according to a letter obtained by The Hill.”*

*“DHS in a letter to Sen. Ron Wyden (D-Ore.) last Monday said they came across unauthorized cell-site simulators in the Washington, D.C., area last year. Such devices, also known as “stingrays,” can track a user’s location data through their mobile phones and can intercept cellphone calls and messages.”*

**05.04.18**

**Reuters**

**[Facebook says data leak hits 87 million users, widening privacy scandal](#)**

Internet giant Facebook have announced that 87 million users’ personal information was shared with software company Cambridge Analytica, who illegally used this data to influence the United States elections.

*“Facebook Inc said on Wednesday that the personal information of up to 87 million users, mostly in the United States, may have been improperly shared with political consultancy Cambridge Analytica, up from a previous news media estimate of more than 50 million.”*

*“Chief Executive Mark Zuckerberg said in a conference call with reporters that Facebook had not seen “any meaningful impact” on usage or ad sales since the scandal, although he added, “it’s not good” if people are unhappy with the company.”*

## Internet Inclusion

**02.04.18**

**The Hill**

### Agencies have one-year deadline to identify cyber workforce shortages

The US Office of Personal Management have announced that they will give federal agencies one year to identify their cybersecurity skills gap in a bid to deal with the ever-growing issue.

*“The Office of Personnel Management (OPM) is giving federal agencies a one-year deadline to identify and report on skill shortages in their cybersecurity workforces.”*

*“A memorandum unveiled Monday requires each agency to tell the government's human resource office what their "critical needs" are in a broad range of cyber workforce areas, including security and information technology.”*

**02.04.18**

**The Times**

### Mars could be swarming with robots

Chang-kwon Kang, of the University of Alabama has been awarded a \$125,000 grant to create a robot-bees with giant wings carrying microcomputers, sensors and wireless communication to explore Mars and prepare for the arrival of human explorers.

*“Robot-bees with giant wings could scout the Red Planet to prepare for the arrival of human explorers, Nasa has revealed.”*

*“The electronic insects, or Marsbees, will be about the size of bumblebees, but with much larger wings in order to manoeuvre in an atmosphere 100 times thinner than Earth's. They will carry microcomputers, sensors and wireless communication devices and will be deployed from a Mars rover vehicle.”*

## Pan-Asia

### Internet governance

**04.04.18**

**Open Gov**

#### [INTERPOL holds first DarkNet and Cryptocurrencies Working Group in Singapore](#)

The International Criminal Police Organisation (INTERPOL) have held a working group meeting of eighteen-member countries including Europol to discuss the DarkNet and Cryptocurrencies in Singapore. The group identified alternative cryptocurrencies as a threat to law enforcement.

*“INTERPOL held the first Working Group on DarkNet and Cryptocurrencies in Singapore. The Working Group identified the rise of Altcoins as an emerging threat to law enforcement.”*

*“Held at the INTERPOL Global Complex for Innovation in Singapore, in cooperation with the German Bavarian Ministry of Justice, the working group gathered 39 participants representing 18-member countries and Europol.”*

**02.03.18**

**The Straits Times**

#### [Anti-Fake News Bill passed in Parliament](#)

An Anti-Fake News Bill has passed the policy stage in the Dewan Rakyat, the lower house of the Parliament of Malaysia. The Bill seeks to stop the spread of fake news by threatening those who spread fake news with six years in prison.

*“The Anti-Fake News Bill 2018 was passed in the policy stage in the Dewan Rakyat today following a bloc vote, following days of heated debate.”*

*“The Bill, which seeks to formulate a new law to stop the spread of fake news which could threaten the country’s political stability and undermine public order and national security, was passed with 123 voting in favour and 64 against.”*

## Cybersecurity

**29.03.18**

### **Security Brief Asia**

#### [Asia's tech-enabled real estate needs to smarten up on cyber risk](#)

A new report on smart cities in the Asia Pacific region has warned that while smart technologies are increasingly being applied to connect urban real estate, infrastructure and services, more cyber protection will be required.

*“As Asia Pacific’s smart cities grow increasingly smarter, they are not necessarily growing more secure.”*

*“Risks associated with tech-enabled real estate and infrastructure will demand more cyber protection, according to a report commissioned by professional services firm JLL and conducted by startup community Tech In Asia.”*

**31.03.18**

### **OpenGov**

#### [ASEAN-Japan Cybersecurity Capacity Building Centre to be launched in Thailand in June 2018](#)

Thailand and Japan are partnering to create an ASEAN-Japan Cybersecurity Capacity Building Centre in Thailand in June this year. 700 cybersecurity personnel will be trained to fight cybercrime in the region.

*“The Centre aims to develop the cybersecurity workforce in ASEAN, particularly in governmental agencies and Critical Information Infrastructure operators in ASEAN, training at least 700 cybersecurity personnel in the region in four years.”*

*“The Ministry of Digital Economy and Society (MDES) of Thailand and Ministry of Internal Affairs and Communications (MIC) of Japan are partnering for the establishment of a ASEAN-Japan Cybersecurity Capacity Building Centre (AJCCBC) in Thailand in June. The Centre is expected to play the key role in mitigating cybercrime in the region as well as getting ready for the establishment of ASEAN-CERT.”*



**03.04.18**

**South China Morning Post**

**[Cybersecurity threats are on the rise in Thailand](#)**

According to Software company, Symantec, cybersecurity threats have worsened in Thailand in 2017 compared to 2016, as more devices were connected and the country took more interest in cryptocurrency and exchanges.

*“Cybersecurity threats in Thailand are intensifying, the country’s ranking dropping last year to 18th-worst from 25th in 2016, with cryptojacking in particular on the rise, says Symantec, a leading information security firm.”*

*“Cybersecurity threats in Thailand worsened in 2017, compared with 2016, because there were more connected devices and higher interest in cryptocurrencies and exchanges,” said Sherif El-Nabawi, senior director for Asia-Pacific system engineering.”*

**04.04.18**

**The Straits Times**

**[LGMS launches Asia Cybersecurity Exchange](#)**

LGMS an IT security services company has launched the Asia Cybersecurity Exchange (AsiaCyberX) which will train 240 cybersecurity specialists and invest RM200 million in technology start-ups that provide cybersecurity services in Malaysia.

*“LE Global Services Sdn Bhd (LGMS) has launched the Asia Cybersecurity Exchange (AsiaCyberX) to propel Malaysia to be a major cybersecurity hub in the borderless realm of the Internet.”*

*“LGMS chief executive officer Fong Choong Fook said AsiaCyberX’s mission is to grow the talent pool for cybersecurity experts and technology start-ups with huge growth potential.”*

**04.04.18**

**The Hill**

**[Chinese cyber spies pose challenge for Trump admin](#)**

The Trump administration is struggling to deal with Chinese cyber spies that continuously hack into US businesses and steal information from defence contractors.

*“Chinese espionage activity is posing a challenge for the Trump administration as it seeks to crack down on China for allegedly unfair trade practices, including persistent cyber intrusions targeting U.S. businesses.”*

*“While China has largely stopped hacking into U.S. companies to steal intellectual property in accordance with a 2015 Obama-era pact, security experts say Beijing’s spies have continued to break into U.S. networks to advance China’s economic and national security ambitions—testing the limits of the deal.”*

## Privacy

**03.04.18**

**Channel NewsAsia**

### [Indonesia warns Facebook of shutdown if privacy breached: Report](#)

Rudiantara Indonesia's Communications and Information Minister said if evidence emerges that internet giant Facebook has not adequately protected their citizens data and failed to tackle fake news in the upcoming election then he will shut them down.

*“Indonesia's communications and information minister Rudiantara has threatened to shut down Facebook in the country if there is evidence of citizens' personal data being harvested or if it fails to tackle fake news in the upcoming elections, Bloomberg reported on Tuesday (Apr 3).”*

*“In an interview with the agency, Mr Rudiantara said: “If I have to shut them down, then I will do it.””*

## Internet Inclusion

**04.04.18**

**The Straits Times**

### [Malaysia set to become world's 24th largest economy by 2050](#)

PwC Malaysia Managing Partner, Sridharan Nair has urged the Government to invest in technology to ensure that Malaysia can improve its ranking even though it is on track to become the 24<sup>th</sup> largest economy by 2050.

*“Malaysia, a medium-sized economy, is expected to improve its ranking to be the 24th largest in the world by 2050.”*

*“PwC Malaysia Managing Partner, Sridharan Nair, said Malaysia, already in the 27th position in terms of gross domestic product (GDP) contribution to the global economy, needed to invest in technology and education to further improve its ranking.”*

## Rest of the World

### Internet governance

**30.03.18**

**The Guardian**

#### [CPN declares war on quacks in IT sector](#)

Computer Professionals (Registration Council of) Nigeria (CPN) have announced that it will now be mandatory for individuals to obtain a licence from the Council before they can engage in IT training, education, use and sale of computing facilities or a computational related role.

*“Computer Professionals (Registration Council of) Nigeria (CPN), said it is now mandatory for all persons and organizations seeking to engage, or engaged in IT training/Education, sale and/or use of computing facilities, and the provision of professional services in computational or related computational machinery in Nigeria to be registered by the Council and licensed to carry out such activities.”*

*“Deriving powers from the Act No 49 of 1993 which established it, CPN said it was also working with the National Information and Technology Development Agency (NITDA) to ensure that IT contractors not registered with it (CPN) are blocked from getting and executing federal governments ICT projects.”*

**04.04.18**

**The Guardian**

#### [ISPON gathers stakeholders to discuss Nigeria’s fourth industry revolution](#)

According to the President of the Institute of Software Practitioners of Nigeria (ISPON) stakeholders will attend an event on April 6 in Lagos to discuss Nigeria’s fourth industrial revolution and how the country can harness technology.

*“Preparation for Nigeria’s 4th industrial revolution will be the centre of discussion at the fourth coming Institute of Software Practitioners of Nigeria (ISPON) President’s Dinner.”*

*“According to President of ISPON, Olorogun James Emadoye, the event, which is scheduled for April 6 in Lagos, has its theme as “The Fourth Industrial Revolution, A Golden Opportunity for Nigeria to leapfrog into the league of developed nations.”*

## Cybersecurity

**04.04.18**

**The Guardian**

### [Cisco wants organisations to tighten noose on ransomware sophistication](#)

American IT company Cisco has urged companies in the Middle East and Africa to adopt tougher security measures, and to educate their workforce to protect their businesses from cyber espionage.

*“As cybercrimes become more rampant and sophisticated, Cisco, the global leader in IT and networking, has called on businesses, especially in Middle East and Africa (MEA) to adopt security measures and to take a comprehensive approach across people, process, technology and policy to protect their businesses from hackers and cyber criminals.”*

*“This follows the findings reported in the recently released Cisco 2018 Annual Cybersecurity Report, which identified the evolution of ransomware as one of the most significant threat developments over the past year.”*

**04.04.18**

**The Guardian**

### [Organisations should prepare against fifth generation cyber-attacks, Voges warns](#)

Andrew Voges, a Threat Prevention Sales Leader at Check Point Software Technologies in the Middle East and Africa said companies in Nigeria need to prepare for fifth generation cyber-attacks such as malware.

*“Andrew Voges is the Threat Prevention Sales Leader, Middle East and Africa at Check Point. He spoke with ADEYEMI ADEPETUN, on the latest trends in global cyberattacks, especially fifth-generation attacks. Excerpts...”*

*“How will you describe the 2017, which saw increase in cyber attacks globally, Nigeria inclusive?”*

## Privacy

**04.04.18**

**Reuters**

### [In Africa, scant data protection leaves internet users exposed](#)

Privacy advocacy groups in Africa have raised concerns for the limited consensus on data protection rules across the continent, warning that this is potentially putting Africa's ever increasing number of internet users at risk.

*"In Kenya, which has a large and fast-growing population of internet users, there are no specific laws or regulations to protect the privacy of those individuals."*

*"Kenya is not alone in Africa, which as a region has clocked the world's fastest growth in internet use over the past decade. Unlike in Europe and the United States, where data-privacy laws provide a level of protection to consumers, many Africans have little or no recourse if a data breach occurs because often legal and regulatory safeguards don't exist."*

**05.04.18**

**Channel News Asia**

### [Australia begins privacy investigation into Facebook](#)

Australia have announced that they will investigate Facebook to assess whether the internet giant has breached the countries privacy laws by allowing the data of 300,000 Australian users to be used without their consent.

*"Australia on Thursday said it had begun an investigation to decide whether social media giant Facebook Inc breached its privacy laws, after the company confirmed data from 300,000 Australian users may have been used without authorisation."*

*"Personal information of up to 87 million users, mostly in the United States, may have been improperly shared with political consultancy Cambridge Analytica, Facebook said on Wednesday, exceeding a media estimate of more than 50 million."*

## Internet Inclusion

**30.03.18**

**The Guardian**

### [Researchers discover technologies to make computers run 100 times faster](#)

Researchers in Israel have used a terahertz microchip to run a computer one hundred times faster than a usual laptop.

*“Israel researchers have reportedly discovered technologies that will enable computer to run 100 times faster through the use of terahertz microchips. The findings were made by Hebrew University of Jerusalem (HU) physicist, Uriel Levy, and his team after three years of research, said sources from the university.”*

*“Now, two major challenges stand in the way of creating the terahertz microchip: overheating and scalability. However, in a paper published in Laser and Photonics Review, Levy, Head of HU’s Nano-Opto Group, and HU emeritus Prof. Joseph Shappir have shown proof of the concept for an optic technology that integrates the speed of optic (light) communications with the reliability of electronics.”*

**29.03.18**

**The Guardian**

### [University of Cape Town now offers FinTech short course for business](#)

The University of Cape Town have announced that they are now offering FinTech courses for businesses in the face of a growing digital skills gap.

*“According to the recent Finnovating for Africa report released by media and research company Disrupt Africa, Africa is already home to more than 300 Fintech startups, having raised almost \$100 million over the last 2.5 years. But the industry is crying out for skilled professionals who understand the technology and are able to capitalise on its potential.”*

*“So says Dr Co-Pierre Georg, Associate Professor at the African Institute of Financial Markets and Risk Management (AIFMRM) at UCT and convener of a brand new course on Facing the Fintech Challenge at the UCT Graduate School of Business (GSB).”*

**03.04.18**

**The Guardian**

**Embracing technology to ensure learners reach their full potential**

Mampho Langa the Head of Future Nation Schools in South Africa said technology can be used in schools to improve learning outcomes by playing online educational games.

*“In an increasingly digital world, where technology continues to enhance literally every touch point in our daily lives, it is within the education sector that its impact can potentially prove most profound.”*

*“This is particularly the case for the African continent where the uptake of mobile devices continues to increase annually.”*



## Global Institutions

**28.03.18**

**ITU**

### [ITU publishes key reports to foster digital transformation](#)

The Internet Telecommunication Union have published several documents to help support ITU member states to promote economic growth and job creation through digital innovation.

*“The International Telecommunication Union (ITU) has launched a series of publications designed to support ITU Member States to promote economic growth and job creation through digital innovation. The publications were launched this month during World Summit on the Information Society Forum 2018 (WSIS 2018).”*

*“The publications now available are: Digital innovation profiles for Bosnia and Herzegovina, and Serbia. The Digital Innovation Profiles (DIP) are part of the ITU's new series of information and communication technology (ICT)-focused innovation ecosystem snapshots, which offer a quick assessment of the existing capacity to accelerate digital transformation and an overview of opportunities and challenges facing the countries' ecosystems.”*

**04.04.18**

**Open Gov**

### [INTERPOL holds first DarkNet and Cryptocurrencies Working Group in Singapore](#)

The International Criminal Police Organisation (INTERPOL) have held a working group meeting of eighteen-member countries including Europol to discuss the DarkNet and Cryptocurrencies in Singapore. The group identified alternative cryptocurrencies as a threat to law enforcement.

*“INTERPOL held the first Working Group on DarkNet and Cryptocurrencies in Singapore. The Working Group identified the rise of Altcoins as an emerging threat to law enforcement.”*

*“Held at the INTERPOL Global Complex for Innovation in Singapore, in cooperation with the German Bavarian Ministry of Justice, the working group gathered 39 participants representing 18-member countries and Europol.”*

## Diary Dates

**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

**Cyber in the Digital Economy – 17.05.18**

London, England

**2018 Digital Festival – 21.05.18**

London, England

**Diversity in Technology – 24.05.18**

London, England

**EuroDIG – 05.06.18-06.06.18**

Tbilisi, Georgia

**Data Centres Risk Radar – 24.06.18**

London, England