21 February 2018

Synopsis

Scroll to read full summaries with links to news articles.

The **Indonesian** Minister of **Communications** said that new **technology** to search **internet content** and issue alerts for harmful materials has blocked more than seventy thousand websites it has deemed 'inappropriate.'

According to the **Internet and Mobile Association** of India & Kantar **IMRB** the number of internet users in **India** will reach half a billion by June this year, however, it remains a largely male dominated sphere.

Researchers, students and teachers across five **Indian** institutes of **Technology** are joining forces to get involved in a **Department of Telecommunications**-backed project which aims to develop 5th generation **mobile networks** technology.

The **United Nations** Secretary General **Antonio Guterres** has urged for global rules and a regulatory scheme to be created for **cyberwarfare**.

The **UK** and **United States** Government have publicly blamed **Russia** for the **NotPetya ransomware** attacks in June 2017.

Facebook has lost a **Belgian privacy** case which means the social media giant could face fines of up to $125 million if it fails to stop tracking people on third party websites.

Addressing the SC Congress, **Peter Brown**, Group Manager at the Information Commissioner's Office warned that it will now become a 'legal minimum' to be compliant with the forthcoming **GDPR** regulations.

The **United States Department for Energy** is creating an office solely dedicated to protecting the countries national power grid and other **infrastructure** against **cyber-attacks**.

Intel have announced that shareholders and customers have filed thirty-two class action **lawsuits** against the technology company after **security flaws** were discovered in their microchips.

Dmitry Peskov, Kremlin's spokesman has publicly denied that **Russia** was involved or responsible for the '**NotPetya'** cyber attacks last year.

According to a new report, **North Korea** is expanding the sophistication and scope of its **cyber weaponry** to commit **cyber espionage** on a large scale.

Australia's Notifiable Data Breaches scheme mandates that the Australian Government and other organisations must notify individuals that are affected by **data breaches** that will result in serious harm.

The **European Internet Forum** has published a document on the future partnership between the **EU** and the **USA** which urged for more clarity on the expanding sphere of **data policy**.

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

21 February 2018

Table of Contents

Europe

Internet governance

No new items of relevance

Cybersecurity

14.02.18

Security Brief Asia

67% of organisations say they're understaffed to handle cybersecurity

According to a survey by cybersecurity company RiskIQ, 67% of US and UK information security organisations do not have enough staff to handle cybersecurity threats.

"There is almost no question that cybercrime is growing in sophistication and distribution every year."

"For instance, you can go straight to the horse's mouth with nearly 90 percent of all information security leaders revealing they're concerned with the rise of digital threats they are facing across web, social, and mobile channels."

16.02.18

SC Media

UK government publicly blames Russia for NotPetya attacks

The UK Government has publicly blamed Russia for the NotPetya ransomware attacks in June 2017 on grounds that the Government will not encourage "malicious cyber-activity."

"The UK government publicly accused Russia of carrying out the June 2017 NotPetya ransomware attacks in June 2017 as part of a deliberate attack on the Ukraine state."

"The decision to publicly blame the Kremlin for the attack was made on the grounds that the government will not tolerate "malicious cyber-activity" Foreign Office Minister of Cyber-security Lord Tariq Ahmad said according to The Daily Telegraph."

19.02.18

Reuters

U.N. chief urges global rules for cyber warfare

The United Nations Secretary General Antonio Guterres has urged for global rules and a regulatory scheme to be created for cyberwarfare.

"U.N. Secretary General Antonio Guterres called on Monday for global rules to minimize the impact of electronic warfare on civilians as massive cyber-attacks look likely to become the first salvoes in future wars."

"Computer hackers, many of them believed to be state-sponsored groups, last year disrupted multinational firms, ports and public services on an unprecedented scale around the world, raising awareness of the issue."

Privacy

15.02.18

Channel NewsAsia

EU tells Facebook, Google and Twitter to do more for users

On Thursday last week, Europe's Justice Commissioner, Vera Jourova, told Google and Facebook to do more to bring their user terms in line with EU Law, after the technology companies faced scrutiny over privacy issues.

"Europe's justice commissioner told Facebook, Twitter and Google on Thursday to do more to bring their user terms in line with EU law, saying proposals submitted by the tech giants were considered insufficient."

"The European Union executive and consumer protection authorities said the three companies have only partially addressed concerns about their liability and how users were informed about content removal or contract terminations."

15.02.18

SC Media

SC Congress 2018 Security best practices needed to stay in line with GDPR

Addressing the SC Congress, Peter Brown, Group Manager at the Information Commissioner's Office warned that it will now become a 'legal minimum' to be compliant with the forthcoming GDPR regulations.

"It's not enough to do the minimum necessary now with enforcement of new rules less than 100 days away. With GDPR coming into force less than 100 days, organisations need to make sure they are using best practices for security now."

"With GDPR coming into force less than 100 days, organisations need to make sure they are using best practices for security now to ensure they comply with forthcoming regulations, rather than meeting the bare minimum that current rules enforce, delegates heard at the SC Congress in London."

16.02.18

Channel News Asia

Facebook loses Belgian privacy case, faces fine up to US$125 million

Facebook has lost a Belgian privacy case which means the social media giant could face fines of up to $125 million if it fails to stop tracking people on third party websites.

"A Belgian court threatened Facebook with a fine of up to 100 million euros (US$125 million) if it continued to break privacy laws by tracking people on third party websites."

19.02.18

European Internet Forum

EIF publishes priorities for a Transatlantic Digital Transformation Agenda

The European Internet Forum has published a document on the future partnership between the EU and the USA which argues for more clarity on the expanding sphere of data policy.

"Re-launching Transatlantic Partnership 2020 - The Digital Dimension"" is an EIF publication produced by EIF's Senior Advisor Peter Linton at the request of the Transatlantic Policy Network (TPN) to create and set the goals for a transatlantic digital transformation agenda."

Internet Inclusion

No new items of relevance

United States of America

Internet governance

No new items of relevance

Cybersecurity

13.02.18

Channel NewsAsia

US Democrats push US$1 billion bill for election security

Congressional Democrats have introduced a Bill that if passed would allocate one billion dollars to make the US voting system cyber resilient.

"Congressional Democrats on Wednesday introduced legislation that would provide more than US$1 billion to boost cyber security of U.S. voting systems, and Vice President Mike Pence defended the administration's efforts to protect polls from hackers."

"The measure followed warnings on Tuesday from U.S. intelligence officials that midterm races in November are likely to see renewed meddling from Russia and possibly other foreign adversaries."

14.02.18

Reuters

U.S. Energy Department forming cyber protection unit for power grids

The United States Department for Energy is creating an office solely dedicated to protecting the countries national power grid and other infrastructure against cyber-attacks.

The U.S. Department of Energy (DOE) said on Wednesday it is establishing an office to protect the nation's power grid and other infrastructure against cyber-attacks and natural disasters.

President Donald Trump's budget proposal unveiled this week included $96 million in funding for the Office of Cybersecurity, Energy Security, and Emergency Response.

14.02.18

Security Brief Asia

67% of organisations say they're understaffed to handle cybersecurity

According to a survey by cybersecurity company RiskIQ sixty-seven per cent of US and UK information security organisations do not have enough staff to handle cybersecurity threats.

"There is almost no question that cybercrime is growing in sophistication and distribution every year."

"For instance, you can go straight to the horse's mouth with nearly 90 percent of all information security leaders revealing they're concerned with the rise of digital threats they are facing across web, social, and mobile channels."

16.02.18

Reuters

Intel hit with 32 lawsuits over security flaws

Intel have announced that shareholders and customers have filed thirty-two class action lawsuits against the technology company after security flaws were discovered in their microchips.

"Intel Corp said on Friday shareholders and customers had filed 32 class action lawsuits against the company in connection with recently-disclosed security flaws in its microchips."

"Most of the lawsuits - 30 - are customer class action cases that claim that users were harmed by Intel's "actions and/or omissions" related to the flaws, which could allow hackers to steal data from computers."

Privacy

15.02.18

Channel NewsAsia

EU tells Facebook, Google and Twitter to do more for users

On Thursday last week, Europe's Justice Commissioner told Google and Facebook to do more to bring their user terms in line with EU Law, after the technology companies faced scrutiny over privacy issues.

“Europe's justice commissioner told Facebook, Twitter and Google on Thursday to do more to bring their user terms in line with EU law, saying proposals submitted by the tech giants were considered insufficient.”

“The European Union executive and consumer protection authorities said the three companies have only partially addressed concerns about their liability and how users were informed about content removal or contract terminations.”

15.02.18

Security Brief Asia

US intelligence agencies accuse Huawei & ZTE of spying - again

United States intelligence agencies have again warned that customers that use products from Chinese technology giant Huawei may be spied on. They failed to share any evidence to support their claims.

“Four United States intelligence agencies are warning that Chinese technology giant Huawei may spy on customers who own Huawei smart devices – but they are not sharing any hard evidence to prove it.”

“At the Senate Intelligence Committee this week, the director of national intelligence, as well as chiefs from the NSA, FBI and CIA warned against organisations including Huawei and ZTE and their efforts to expand into the United States market.”

16.02.18

Channel News Asia

Facebook loses Belgian privacy case, faces fine up to US$125 million

Facebook has lost a Belgian privacy case which means the social media giant could face fines of up to $125 million if it fails to stop tracking people on third party websites.

“A Belgian court threatened Facebook with a fine of up to 100 million euros (US$125 million) if it continued to break privacy laws by tracking people on third party websites.”

“In a case brought by Belgium's privacy watchdog, the court also ruled on Friday that Facebook had to delete all data it had gathered illegally on Belgian citizens, including people who were not Facebook users themselves.”

19.02.18

European Internet Forum

EIF publishes priorities for a Transatlantic Digital Transformation Agenda

The European Internet Forum has published a document on the future partnership between the EU and the USA which urged for more clarity on the expanding sphere of data policy.

"Re-launching Transatlantic Partnership 2020 - The Digital Dimension"" is an EIF publication produced by EIF's Senior Advisor Peter Linton at the request of the Transatlantic Policy Network (TPN) to create and set the goals for a transatlantic digital transformation agenda."

"This contribution serves as one of four reports, alongside inputs focused on the political, economic and security dimensions of future Transatlantic partnership. Unsurprisingly, each of these three analyses likewise reflects the growing impact of digital technologies and capabilities."

Internet Inclusion

17.02.18

Gadgets Now

Facebook forges ahead with kids app despite expert criticism

Facebook is pressing ahead with its messaging app designed for children, despite widespread concern that it could lure kids into harmful social media use.

"Facebook is forging ahead with its messaging app for kids, despite child experts who have pressed the company to shut it down and others who question Facebook's financial support of some advisers who approved of the app."

"Messenger Kids lets kids under 13 chat with friends and family. It displays no ads and lets parents approve who their children message. But critics say it serves to lure kids into harmful social media use and to hook young people on Facebook as it tries to compete with Snapchat or its own Instagram app. They say kids shouldn't be on such apps at all _ although they often are."

17.02.18

Channel NewsAsia

N.Y. judge says Charter must face lawsuit over slow internet

Charter Communications an American telecommunications company has been accused of providing customers with slower than advertised internet speeds and is now facing a lawsuit by New York's Attorney General.

"Charter Communications Inc must face a lawsuit by New York's attorney general accusing the cable company of giving customers slower-than-advertised internet speeds, a New York state judge ruled in a decision made public on Friday."

"Justice O. Peter Sherwood of state Supreme Court in Manhattan rejected Charter's claim that Attorney General Eric Schneiderman failed to plausibly allege it had short-changed and misled customers. He also rejected Charter's claim that federal law pre-empted the lawsuit."

Pan-Asia

Internet governance

19.02.18

Gadgets Now

New Indonesia web system blocks more than 70,000 'negative' sites

The Indonesian Minister of Communications said that new technology to search internet content and issue alerts for harmful materials has blocked more than seventy thousand websites it has deemed 'inappropriate.'

"Indonesia has blocked more than 70,000 websites displaying "negative" content such as pornography or extremist ideology in the first month of using a new system to help purge the internet of harmful material, the communications minister told Reuters."

"The world's most populous Muslim-majority country has stepped up efforts to control online content after a rise in hoax stories and hate speech, and amid controversial anti-pornography laws pushed by Islamic parties."

Cybersecurity

14.02.18

Security Brief Asia

Cyber warfare market to be worth $120b by 2025 as national security concerns intensify

According to a report from a U.S. based market research and consulting company Grand View Research, the global cyber warfare market may be worth $120 billion by 2025 and Asia Pacific will be the fastest growing region in the world.

"The global cyber warfare market may be worth S$120 billion by 2025 and Asia Pacific will be the fastest-growing region in the world, according to a report from Grand View Research."

"The market growth is being driven by concern about the 'catastrophic nature' of cyber warfare and national security, both of which are being plagued by cyber attackers intent on disrupting economic growth and stealing defense force IP."

18.02.18

This Week and Asia

Can Indonesia's new cybercrime unit win its war on fake news?

The recently established Indonesian National Cyber and Encryption Agency currently has no operational budget to fight cybersecurity however it has requested three trillion Indonesian Rupiah from Parliament.

"Indonesia has unleashed a new cyber and encryption agency as a weapon in its long war on cybercrime, online radicalism and fake news, but the Southeast Asian nation still needs to define the office's scope of authority to prevent bureaucratic overlap and to shake off privacy concerns."

"A plan to establish the National Cyber and Encryption Agency (BSSN) was put forth four years ago when President Joko Widodo took office, but the agency only started work in January after Major General Djoko Setiadi was installed as its leader."

Privacy

15.02.18

Security Brief Asia

US intelligence agencies accuse Huawei & ZTE of spying - again

United States intelligence agencies have again warned that customers that use products from Chinese technology giant Huawei may be spied on. They failed to share any evidence to support their claims.

"Four United States intelligence agencies are warning that Chinese technology giant Huawei may spy on customers who own Huawei smart devices – but they are not sharing any hard evidence to prove it."

"At the Senate Intelligence Committee this week, the director of national intelligence, as well as chiefs from the NSA, FBI and CIA warned against organisations including Huawei and ZTE and their efforts to expand into the United States market."

Internet Inclusion

17.02.18

Gadgets Now

5 IITs, over 200 researchers are working on a 5G project that may change internet in India

Researchers, students and teachers across five Indian institutes of Technology are joining forces to get involved in a Department of Telecommunications-backed project which aims to develop 5th generation mobile networks technology.

"More than 200 researchers, students and teachers from across five Indian Institutes of Technology have joined forces over a Rs 300-crore project to develop 5G technology and its use cases in India."

"The department of telecommunications-backed project, being billed as the biggest collaborative effort between these institutes, will aim to develop a comprehensive test-bed for 5G that can be used by technology companies, telecom operators, academics and start-ups for R&D purposes and developing 5G products and solutions."

17.02.18

Gadgets Now

Telecom subscribers in India reach 1.19 billion in December 2017: Trai

In a monthly subscribers report the Telecom Regulatory Authority of India announced that nearly eight million new telephone subscribers were recorded in December 2017.

"Telecom subscriber base in India reached 1.19 billion at the end of December 2017 with Reliance Jio adding over 8 million new customers alone during the month, according to data published by telecom regulator Trai.

"The number of telephone subscribers in India increased from 1,185.88 million at the end of November 2017 to 1,190.67 million at the end of December 2017, thereby showing a monthly growth rate of 0.4 per cent," Trai said in a monthly subscribers' report."

19.02.18

Gadgets Now

PM Narendra Modi launches "Futureskills' platform for IT professionals

The Indian Prime Minister applauded Nasscom the trade association of India's IT plans to train two million technology professionals, two million potential employees and students over the next few years.

"Prime Minister Narendra Modi today unveiled Nasscom's 'Futureskills' platform for IT professionals. Modi launched the platform via video conference during the inaugural session of the World Congress on Information Technology (WCIT)-2018 being held in Hyderabad."

"The National Association of Software and Services Companies' (NASSCOM) platform offers skills development in eight different technologies – starting with AI. The other technologies include virtual reality, robotic process automation, Internet of Things (IoT), Big Data Analytics, 3D Printing, Cloud Computing, Social and Mobile."

18.02.18

Channel NewsAsia

Commentary: The hidden value of learning how to code

An expert from the Singapore Management University stressed the importance of Singaporean children learning to code claiming it is essential for the future development of the country.

"In a multilingual Singapore, people see benefits in being fluent in multiple languages."

"Any school-going child in Singapore would probably be well-exposed to the pressures of learning to be effectively bilingual. Chances are, they'll be encouraged profusely by well-meaning parents to live and breathe English as well as Chinese, Malay or Tamil."

20.02.18

Gadgets Now

[Internet in India remains a male dominated space as user base set to touch half a billion: IAMAI]

According to the Internet and Mobile Association of India & Kantar IMRB the number of internet users in India will reach half a billion by June this year, however, it remains a largely male dominated sphere.

“The number of internet users in India will touch half-a-billion by June this year, according to the report 'Internet in India 2017' published jointly by the Internet and Mobile Association of India & Kantar IMRB today.”

“The number of internet users in India was estimated to be 481 million in December 2017, a growth of 11.34% over December 2016. The number of internet users is expected to reach 500 million by June 2018, claims the report.”

Rest of the World

Internet governance

No new items of relevance

Cybersecurity

18.02.18

Channel NewsAsia

Kremlin rejects US accusation that Russia is behind cyber attack

Dmitry Peskov, Kremlin's spokesman has publicly denied that Russia was involved or responsible for the 'NotPetya' cyber-attacks last year.

"Kremlin spokesman Dmitry Peskov said on Friday he denies Russia was responsible for the 'NotPetya' cyber-attack last year, after the White House on Thursday joined the British government in accusing Moscow of the attack."

"In response to a question about the attack, he said he reiterated comments made on Thursday, when he said that the allegations by a British official about 'NotPetya' attack were groundless and part of a "Russophobic" campaign being conducted in some Western countries."

16.02.18

SC Media

UK government publicly blames Russia for NotPetya attacks

The UK Government has publicly blamed Russia for the NotPetya ransomware attacks in June 2017 on grounds that the Government will not encourage "malicious cyber-activity."

"The UK government publicly accused Russia of carrying out the June 2017 NotPetya ransomware attacks in June 2017 as part of a deliberate attack on the Ukraine state."

"The decision to publicly blame the Kremlin for the attack was made on the grounds that the government will not tolerate "malicious cyber-activity" Foreign Office Minister of Cyber-security Lord Tariq Ahmad said according to The Daily Telegraph."

20.02.18

The Straits Times

North Korea poised to launch large-scale cyber-attacks, says new report

According to a new report North Korea is expanding the sophistication and scope of its cyber weaponry to commit cyber espionage on a large scale.

"North Korea is quietly expanding both the scope and sophistication of its cyber weaponry, laying the groundwork for more devastating attacks, according to a new report published on Tuesday (Feb 20)."

"Kim Jong Un's cyber warriors have been accused of causing huge disruption in recent years, including being blamed for the massive hack on Sony Pictures in 2014 and last year's WannaCry ransomware worm, as well as umpteen attacks on South Korean servers."

Privacy

20.02.18

Open Gov

Australia's Notifiable Data Breaches scheme commencing on February 22

Australia's Notifiable Data Breaches scheme which will come into effect on February 22, 2018, mandates that the Australian Government and other organisations must notify individuals that are seriously harmed by data breaches.

"The NDB scheme mandates that Australian Government agencies and the various organisations with obligations to secure personal information under the Privacy Act 1988 notify individuals affected by data breaches that are likely to result in serious harm."

"Australia's Notifiable Data Breaches (NDB) scheme will come into effect later this week on February 22, 2018. Ahead of the commencement, the Office of the Australian Information Commissioner (OAIC) has released new resources for the Australian public."

Internet Inclusion

14.02.18

The Guardian

MainOne plans IT stakeholder summit for third year

MainOne, West Africa's connectivity and datacentre provider is planning an IT stakeholder summit which will bring together five hundred ICT executives to discuss cybersecurity and emerging threats.

"MainOne will for the third-time host ICT stakeholders at its yearly flagship event, Nerds Unite."

"With a focus on digital disruption with the theme 'Radical Digital Transformation', the 2018 edition will feature a keynote address from the author of Disrupting Africa: The Rise & Rise of African Innovation, Nnamdi Oranye supported by speakers from companies including Avanti, SAP Africa, Wema Bank, Andela and Microsoft among many others."

20.02.18

The Guardian

NAF urges personnel to acquire ICT

The Nigerian Chief of Air Staff, Air Marshal Sadique Abubakar has urged personnel to acquire Information Communication Technology to make operations more efficient.

"The Chief of Air Staff (CAS), Air Marshal Sadique Abubakar, has charged its personnel to acquire Information Communication Technology (ICT) in line with global trends."

"He made the call in Abuja, at the 2018 Nigerian Air Force Branch Workshop, titled: "Positioning communications branch for effective, efficient and timely support of NAF operations."

Global Institutions

19.02.18

Reuters

U.N. chief urges global rules for cyber warfare

The United Nations Secretary General Antonio Guterres has urged for global rules and a regulatory scheme to be created for cyberwarfare.

"U.N. Secretary General Antonio Guterres called on Monday for global rules to minimize the impact of electronic warfare on civilians as massive cyber-attacks look likely to become the first salvoes in future wars."

"Computer hackers, many of them believed to be state-sponsored groups, last year disrupted multinational firms, ports and public services on an unprecedented scale around the world, raising awareness of the issue."

19.02.18

European Internet Forum

EIF publishes priorities for a Transatlantic Digital Transformation Agenda

The European Internet Forum has published a document on the future partnership between the EU and the USA which urged for more clarity on the expanding sphere of data policy.

"Re-launching Transatlantic Partnership 2020 - The Digital Dimension"" is an EIF publication produced by EIF's Senior Advisor Peter Linton at the request of the Transatlantic Policy Network (TPN) to create and set the goals for a transatlantic digital transformation agenda."

"This contribution serves as one of four reports, alongside inputs focused on the political, economic and security dimensions of future Transatlantic partnership. Unsurprisingly, each of these three analyses likewise reflects the growing impact of digital technologies and capabilities."

Diary Dates

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

EuroDIG – 05.06.18-06.06.18

Tbilisi, Georgia