23 August 2018

Synopsis

Scroll to read full summaries with links to news articles.

Amidst a clamp down on online content on livestreams, blogs and mobile gaming, Chinese President **Xi Jinping** declared that the internet must be 'clean and righteous. **China** shut as many as 128,000 websites that contained 'obscene and other harmful' information in 2017 as it seeks to maintain its grip over the **internet** which is popular with China's youth.

The **European Commission** consider that **social media** companies have not done enough to remove illegal and terrorist content from their platforms in a three-month reporting period and will seek to levy harsh fines if **content** is not removed within an hour.

President Trump has rescinded an Obama era **Presidential Policy Directive** to enable the military to conduct **cyber operations** without requiring high-level approval or interagency discussions.

Campaigners are calling for **Google** to face fines under **GDPR** rules which prohibits **tracking** without proper **consent** or legitimate purpose. It comes after revelations that location tracking continues when the user *thinks* they have disabled it.

Australia has joined the **US** in banning major telecoms firm **Huawei** from supplying equipment to its **5G** mobile network. The Australian Government issued a statement saying 'suppliers "who are likely to be subject to extrajudicial directions from a foreign government" would leave Australia's network vulnerable to unauthorised access or interference.'

During a meeting with Singapore's **CSA**, **Asean** nations were asked to tighten their cooperation on **cybersecurity** to prevent internet crime as **Singapore** seek to develop a rules based order for **cyberspace** in the region.

Following the **SingHealth** breach where records of 1.5 million patients were breached, the **CSA** has sought to strengthen the defenses of critical information infrastructure. 11 critical service sectors have been asked to review their connections to 'untrusted external networks.'

The number of **internet users** in **China** has risen by 30 million in the first half of 2018. The total number of Chinese internet users is now over 800 million with 566 million of these using mobile payments. As the market increases so too does commercial opportunity but also the risk of illegal content.

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

22 August 2018

Table of Contents

Europe

Internet governance

20.08.18

Computing

EU demands that internet companies take down illegal and 'terrorist content' down within an hour - or face harsh fines

The European Commission consider that social media companies have not done enough to remove illegal and terrorist content from their platforms in a three-month reporting period and will seek to levy harsh fines if content is not removed within an hour.

"The European Union is planning on levying harsh fines on social media networks that fail to take down on what it regards as illegal and terrorist content within an hour.

Julian King, the EU's commissioner for security, claimed that self-regulation had failed and that the European Commission therefore needed to take firmer action against social media companies."

14.08.18

Information Age

The EU Copyright Directive: seeing the funny side?

Debate continues around the EU Copyright Directive with legislators planning to bring a revised version of the bill back to Parliament, after the European Parliament originally voted down the proposal.

"Earlier in the summer, the European Parliament voted down the EU's proposed Copyright Directive. The Directive was aimed at providing greater protection for copyright owners by putting the onus on websites and information service providers to take down copyright infringing material. Under the Directive, ISPs would have been obliged to take 'appropriate and proportionate' measures to ensure that uploaded content does not infringe the copyright of third parties."

"Despite voting the Directive down, the debate rages on, and legislators will bring a revised version of the bill back before the Parliament in September."

Cybersecurity

14.08.18

Politico

Central bankers warn of chaos in a cashless society

The cyber attacks associated with digital payment have prompted European central bankers to argue against the introduction of a purely cashless society. 80 per cent of transactions in the Eurozone are still made in cash although in some states such as Sweden just 13 per cent of transactions made in cash.

"Europe's central bankers are warning that a gradual phase-out of cash in many countries poses a serious threat to the financial system, as relying too heavily on digital payment systems exposes them to catastrophic failures in the event of cyberattacks.

Regulators are also weighing in to say that IT failures, systemic hacking risks — and the fact that more vulnerable members of society would be alienated in a cashless world — all argue in favor of keeping a robust system in place — i.e., cash."

Privacy

22.08.18

Computer Weekly

Nearly a third of organisations still not GDPR ready

Whilst most companies claim they are able to respond to data subject access requests, nearly a fifth of organizations are not confident of passing their first GDPR audit and 28 per cent do not feel as if they are compliant with GDPR.

"Some 28% of organizations do not feel completely compliant with the EU's General Data Protection Regulation (GDPR), a survey has revealed.

The UK was among the first countries to introduce GDPR-aligned data protection legislation, so any organizations that are not fully GDPR-compliant are likely to be not fully compliant with the UK Data Protection Act 2018."

16.08.18

The Register

Google risks megafine in EU after location 'stalking'

Campaigners are calling for Google to face fines under GDPR rules which prohibits tracking without proper consent or legitimate purpose. It comes after revelations that location tracking continues when the user *thinks* they have disabled it.

"Privacy campaigners say Google's obsessive collection of location markers violates Europe's privacy laws - potentially exposing the Californian giant to punitive fines."

"Several privacy watchers agree that as it stands, users are misled, and can't give informed consent. That exposes the company to financial penalty under GDPR rules: which could be 2 per cent or 4 per cent of turnover."

20.08.18

The Parallax

How a European Commission antitrust ruling could impact Android privacy

Following a fine of 4.34 billion euros, Google may be restricted from controlling which internet browsing apps are preinstalled on Android devices and from banning the shipping of devices with unapproved alternatives.

"The threat of billions of dollars in European Commission antitrust fines could force Google, in the very near future, to give phone makers a chance to make Android far more respectful of consumer privacy.

In fining Google 4.34 billion euros, or $5.08 billion, for abusing its market power, the European Commission is requiring the Silicon Valley powerhouse to change basic rules associated with its mobile operating system within 90 days. If it doesn't make those changes, it stands to get socked with extra penalties of up to 5 percent of the global revenue of its parent company, Alphabet, which reached $32.7 billion in the second quarter."

Internet Inclusion

22.08.18

Government Europa

UK names three universities cybersecurity research centres of excellence

The UK has continued recognizing universities as research centres of excellence due to contributions to developing digital skills. Status as a centre of excellence enables universities to bid for funding to undertake research into cybersecurity.

"The UK's National Cyber Security Centre and Engineering and Physical Sciences Research Council have recognised the University of Kent, King's College London and Cardiff University as academic centres of excellence in cybersecurity research because of their contributions to developing digital skills."

"The two bodies have now recognised 17 universities across the UK as capable of carrying out first-rate research into cybersecurity as part of the country's national strategy, which aims to utilise the expertise of each of these research institutions to secure the country's digital economy."

16.08.18

IT Pro

A-level results day 2018: University uptake for STEM subjects flat despite more A-level entries

Whilst the number of STEM-related subjects taken at A-level had increased from 34.5% to 36.2% since last year, the number of students accepted onto STEM undergraduate courses stagnated, although computer science saw a 3% rise in entries.

"The number of students accepted onto undergraduate STEM courses between 2017 and 2018 was flat, despite a rise in A-level entries for science and computing subjects.

IT Pro analysis of figures released by UCAS show the number of 'placed applicants' – students accepted onto undergraduate courses – for science and technology subjects fell slightly since last year; from 111,820 in 2017 to 111,360 this year – a 0.004% decline."

21.08.18

Computer Weekly

Estonia targets UK tech talent

The Estonian government has introduced legislation, and policies to address its country's needs and has now established a recruitment campaign targeting IT professionals in the UK advertising roles at Taxify, Twilio, Microsoft, Skype and Swedbank in Estonia.

"The Estonian government is directly targeting IT professionals in the UK through a recruitment campaign that it hopes will help to close an imminent skills gap in the Baltic country."

"Estonia has a population of just 1.3 million and a growing IT sector. By 2020, the country's job market is expected to be short of 37,000 IT professionals."

United States of America

Internet governance

16.08.18

Ars Technica

Ajit Pai knew DDoS claim was false in January, says he couldn't tell Congress

Ajit Pai acknowledged during a Senate Commerce Committee hearing that the FCC previously made false statements Congress. Pai claimed he could not correct the false statement made as he had been informed that the matter was under investigation by the Office of Inspector General.

"The Federal Communications Commission chairman has known that his agency's claims about being hit by DDoS attacks were false for more than six months, but he says he could not correct the record publicly because of an internal investigation that didn't wrap up until this month."

"The FCC Office of Inspector General (OIG) issued its report on the matter last week, finding that the FCC lied to Congress when it claimed that DDoS attacks caused a May 2017 outage that temporarily prevented net neutrality supporters from filing comments opposing Pai's plan to kill net neutrality rules. The false claims were made primarily by former Chief Information Officer David Bray, and Bray's false statements were sent to Congress in attachments to letters that Pai wrote to lawmakers."

17.08.18

Reuters

U.S. Government seeks Facebook help to wiretap Messenger

The U.S. Government is seeking new powers for law enforcement to listen to voice conversations through Facebook's 'Messenger' app to assist in criminal probes. Facebook is contesting the DoJ's demand and the case is being heard in a California court.

"The U.S. government is trying to force Facebook Inc (FB.O) to break the encryption in its popular Messenger app so law enforcement may listen to a suspect's voice conversations in a criminal probe, three people briefed on the case said, resurrecting the issue of whether companies can be compelled to alter their products to enable surveillance."

"The previously unreported case in a federal court in California is proceeding under seal, so no filings are publicly available, but the three people told Reuters that Facebook is contesting the U.S. Department of Justice's demand."

13.08.18

The Verge

Trump signs bill banning Government use of Huawei and ZTE tech

Government use of Huawei and ZTE components or services that are "essential" or "critical" to the systems have been banned in the Defense Authorization Act. The ban goes into effect over the next two years.

"Huawei and ZTE technology will largely be banned from use by the US government and government contractors. The ban was signed into placed by President Trump today as a component of the much larger Defense Authorization Act."

"This caps off months of will-they-won't-they from Republicans, many of whom view the two major Chinese telecoms as national security threats. In June, the Senate overwhelmingly passed an amendment that would have reinstated a trade ban on ZTE, potentially shutting down the company. The House, however, did not, and the big question was how the two chambers would find a compromise — or if they would drop the matter entirely."

Cybersecurity

16.08.18

Politico

Trump scraps Obama rules on cyberattacks, giving military a freer hand

President Trump has rescinded an Obama era Presidential Policy Directive to enable the military to conduct cyber operations without requiring high-level approval or interagency discussions.

"President Donald Trump has eliminated rules governing the process for launching cyberattacks, giving the military freer rein to deploy its advanced hacking tools without pushback from the State Department and the intelligence community, an administration official told POLITICO.

Trump's decision, the latest example of his desire to push decision-making authority down the chain of command, could empower military officials to launch more frequent and more aggressive cyberattacks against adversaries like Russia and Iran."

17.08.18

SC Magazine

[President signs NIST Small Business Cybersecurity Act into law]

A new law giving small businesses the tools to firm up their cybersecurity infrastructure to fight online attacks has been signed into law by President Trump.

"A year and nearly four months after the measure was introduced, the NIST Small Business Cybersecurity Act officially passed after President Donald Trump signed the legislation into law.

Originally proposed as H.R. 2105 in April 2017, the act was later absorbed into U.S. federal law S.770, and requires the director of the National Institute of Standards and Technology, within within one year of the law's passing, to issue guidance and a consistent set of resources to help SMBs identity, assess and reduce their cybersecurity risks."

21.08.18

Computer Weekly

[Microsoft announces free election cyber defence tools]

Microsoft has launched its 'Defending Democracy Program' in an attempt to protect campaigns to increasing political advertising transparency, and to defend against disinformation campaigns.

"Microsoft has announced it will provide "state of the art" cyber security protection at no extra cost to all election candidates and campaign offices using Office 365."

"The initiative, dubbed AccountGuard, is part of Microsoft's Defending Democracy Program and offers protection for candidates and campaign offices at federal, state and local level, as well as think tanks and political organisations under attack."

22.08.18

Channel NewsAsia

[Facebook, Twitter dismantle disinformation campaigns tied to Iran and Russia]

Social media platforms have removed accounts connected to two separate propaganda campaigns, one from Iran and one from Russia. Cybersecurity firm FireEye said Iran's campaign used a network of fake news websites and fraudulent social media personas spread across social media to push narratives in line with Tehran's interests.

"Facebook Inc., Twitter Inc. and Alphabet Inc. collectively removed hundreds of accounts tied to an alleged Iranian propaganda operation on Tuesday, while Facebook took down a second campaign it said was linked to Russia."

"Facebook CEO Mark Zuckerberg said the accounts identified on his company's platform were part of two separate campaigns, the first from Iran with some ties to state-owned media, the second linked to sources which Washington has previously named as Russian military intelligence services."

21.08.18

Reuters

[U.S. imposes fresh sanctions for Russian cyber-related activity]

The U.S has imposed new sanctions on two individuals and two businesses which had attempted to help a further business circumvent previous U.S sanctions.

"The United States on Tuesday imposed sanctions on two Russians, one Russian company and one Slovakian company for what Washington said were their actions to help another Russian company avoid sanctions over the country's malicious cyber-related activities."

"The U.S. Treasury said in a statement that the sanctioned companies, Saint Petersburg-based Vela-Marine Ltd and Slovakia-based Lacno S.R.O., and the two individuals helped Divetechnoservices evade previously imposed sanctions."

Privacy

20.08.18

Reuters

Lawsuit says Google tracks Phone users regardless of privacy settings

Google have been accused of tracking iPhone and Android users even if privacy settings have been changed to prevent it. The plaintiff is seeking damages for Google's 'alleged intentional violations of California privacy laws, and intrusion into people's private affairs'.

"Google has been accused in a lawsuit of illegally tracking the movements of millions of iPhone and Android phone users even when they use a privacy setting to prevent it."

"According to a complaint filed late Friday, Google falsely assures people they won't be tracked if they turn the "Location History" feature on their phones to "off," and instead violates their privacy by monitoring and storing their movements."

16.08.18

The Register

Google risks megafine in EU after location 'stalking'

Campaigners are calling for Google to face fines under GDPR rules which prohibits tracking without proper consent or legitimate purpose. It comes after revelations that location tracking continues when the user *thinks* they have disabled it.

"Privacy campaigners say Google's obsessive collection of location markers violates Europe's privacy laws - potentially exposing the Californian giant to punitive fines."

"Several privacy watchers agree that as it stands, users are misled, and can't give informed consent. That exposes the company to financial penalty under GDPR rules: which could be 2 per cent or 4 per cent of turnover."

20.08.18

The Parallax

How a European Commission antitrust ruling could impact Android privacy

Following a fine of 4.34 billion euros, Google may be restricted from controlling which internet browsing apps are preinstalled on Android devices and from banning the shipping of devices with unapproved alternatives.

"The threat of billions of dollars in European Commission antitrust fines could force Google, in the very near future, to give phone makers a chance to make Android far more respectful of consumer privacy.

In fining Google 4.34 billion euros, or $5.08 billion, for abusing its market power, the European Commission is requiring the Silicon Valley powerhouse to change basic rules associated with its mobile operating system within 90 days. If it doesn't make those changes, it stands to get socked with extra penalties of up to 5 percent of the global revenue of its parent company, Alphabet, which reached $32.7 billion in the second quarter."

13.08.18

NextGov

How California is improving cyber threat information sharing

Governor Jerry Brown's Cal-SCIC initiative seeks to prioritize cyber threats to the public sector with desires to expand into the private sector, which is largely protective of its data.

"*The state wants to add every city and county government to its automated threat feed program in the next three to four years."*

"The California Cybersecurity Integration Center alerted its partners to the Thomas Fire along Interstate 5, before the largest wildfire in the state's modern history was phoned in last December. Someone had taken to Twitter to first report the blaze, and Cal-CSIC's media scrapers—which plug into its automated threat feed—noticed."

18.08.18

Channel NewsAsia

US tech giants plan to fight India's data localisation plans

Last month the Indian main government committee on data privacy proposed a draft law placing a restriction on data flows and for all "critical personal data" to be processed within India. US tech giants such as Amazon and Microsoft attempting to push back against the draft law.

"United States technology giants plan to intensify lobbying efforts against stringent Indian data localisation requirements, which they say will undermine their growth ambitions in India, sources told Reuters."

"US trade groups, representing companies such as Amazon, American Express and Microsoft, have opposed India's push to store data locally."

Internet Inclusion

20.08.18

Computer Weekly

Gartner recommends CIOs get skilled up on deep learning

With emerging technologies such as deep learning and virtual assistants becoming mainstream within the next two to five years CIOs will be required to upskill their workforce for a seamless integration.

"Smart dust, brain controlled computers and general artificial intelligence (AI) are among the technologies that could have an impact on IT in the not too distant future, according to Gartner's Hype Cycle for Emerging Technologies, 2018 research."

"Business and technology leaders will continue to face rapidly accelerating technology innovation that will profoundly impact the way they engage with their workforce, collaborate with their partners, and create products and services for their customers," said Mike J. Walker, research vice-president at Gartner."

Pan-Asia

Internet governance

22.08.18

Channel News Asia

China's Xi says internet must be 'clean and righteous'

Amidst a clamp down on online content on livestreams, blogs and mobile gaming, Chinese President Xi Jinping declared that the internet must be 'clean and righteous. China shut as many as 128,000 websites that contained 'obscene and other harmful' information in 2017 as it seeks to maintain its grip over the internet which is popular with China's youth.

"The internet must be "clean and righteous" and vulgar content must be resisted in the field of culture, Chinese President Xi Jinping told a meeting of senior propaganda officials, state media said on Wednesday (Aug 22).

The government has been tightening controls over internet content as part of what it says are efforts to maintain social stability, taking on "vulgar" and pornographic content as well as the unauthorised dissemination of news."

Cybersecurity

17.08.18

Fifth Domain

China is hacking the same countries it trades with

A cybersecurity research firm has reported that China 'snooped' on its trading partner Kenya and was "aggressively scanning" a swath of Kenyan internet providers, telecommunications companies, government agencies and education networks.

"At the United Nations headquarters in Nairobi, Kenya, bands of marauding monkeys often climb over the towering fences and roam the acres of closely mowed grass. But this June, another type of uninvited guest entered the U.N. premises."

"Equipment located thousands of miles away at Tsinghua University, in the heart of Beijing, China, began to probe the U.N. networks in Kenya, according to research by Recorded Future, a cybersecurity research firm. The researchers observed "network reconnaissance activities," originating from the Tsinghua servers."

21.08.18

Open Gov Asia

Reserve Bank of India Chief: operators should make no compromise on cyber security

After malware attack resulted in Cosmos Co-operative Bank losing $13.5 million, Governor of the Reserve Bank of India, Urjit Patel stated that security should not be taken lightly, corners should not be cut and warned that 'we are only as strong as our weakest link.'

"Last week, Pune-based Cosmos Co-operative Bank lost IN ₹94 crores (approximately US $13.5 million) in a coordinated cyber-attack consisting of thousands of online transactions, through a malware attack on the bank's server."

"The Governor of the Reserve Bank of India, Mr Urjit Patel said that operators in the payments system space should ensure that no corners are cut when it comes to cybersecurity."

16.08.18

Straits Times

Cyber attacks likely as KL govt reviews projects: Security firm

Security firm FireEye said it had found indications of an increase in cyber espionage activity with China based groups seeking to gain information on BRI projects in South East Asia.

"Chinese state-sponsored hackers may be targeting companies and state agencies in Malaysia as it looks to review several major projects linked to China's Belt and Road Initiative (BRI), cyber security firm FireEye said yesterday."

"Malaysian Prime Minister Mahathir Mohamad, who took power after an election win in May, will be in China tomorrow seeking to renegotiate and possibly cancel billions of dollars worth of Chinese-invested projects authorised by his predecessor, Najib Razak."

18.08.28

Straits Times

Singapore ramps up efforts to secure cyber defences

Following the SingHealth breach where records of 1.5 million patients were breached, the CSA has sought to strengthen the defences of critical information infrastructure. 11 critical service sectors have been asked to review their connections to 'untrusted external networks.'

"Efforts to secure the cyber defences of 11 critical service sectors have been put in high gear following the SingHealth data breach, The Straits Times has learnt."

"While the legislative regime to protect the computer systems of these sectors from attacks is to take shape by the end of the year, the Cyber Security Agency (CSA) has already issued prescriptions to strengthen their defences."

17.08.18

The Nation

Singapore calls for Asean cooperation in cybersecurity

During a meeting with Singapore's CSA, Asean nations were asked to tighten their cooperation on cybersecurity to prevent internet crime as Singapore seek to develop a rules based order for cyberspace in the region.

"During the week-long 9th Asean Journalists' Visit Programme in Singapore, 13 journalists from Asean nations were briefed by agency staff on cyber security to promote security within their own workplaces."

"CSA Deputy Chief Executive (Operations) Mr Ng Hoo Ming told the visiting group they were working with cyber security sectors in Asean by sharing experiences at the regional meeting. But some agencies had not sent enough representatives to the meeting so the CSA hoped that more agencies would participate and share lessons learnt in order to bolster cyber security in Asean."

13.08.18

The Verge

[Trump signs bill banning Government use of Huawei and ZTE tech]

Government use of Huawei and ZTE components or services that are “essential” or “critical” to the systems have been banned in the Defense Authorization Act. The ban goes into effect over the next two years.

“Huawei and ZTE technology will largely be banned from use by the US government and government contractors. The ban was signed into placed by President Trump today as a component of the much larger Defense Authorization Act.”

“This caps off months of will-they-won’t-they from Republicans, many of whom view the two major Chinese telecoms as national security threats. In June, the Senate overwhelmingly passed an amendment that would have reinstated a trade ban on ZTE, potentially shutting down the company. The House, however, did not, and the big question was how the two chambers would find a compromise — or if they would drop the matter entirely.”

23.08.18

Channel NewsAsia

[Australia bans China’s Huawei from mobile network build over security fears]

Australia has joined the US in banning major telecoms firm Huawei from supplying equipment to its 5G mobile network. The Australian Government issued a statement saying ‘suppliers “who are likely to be subject to extrajudicial directions from a foreign government” would leave Australia's network vulnerable to unauthorised access or interference’

“Australia's government on Thursday (Aug 23) banned major Chinese telecoms firm Huawei Technologies from supplying equipment for its planned 5G mobile network, citing risks of foreign interference.

Huawei's involvement in the network rollout, and resistance to it from Australia's security agencies, has become a flashpoint between the trading partners in recent months as a row over alleged Chinese meddling in Australian politics deepened.”

Privacy

21.08.18

Channel NewsAsia

WhatsApp to clamp down on 'sinister' messages in India: IT Minister

After a meeting between WhatsApp Chief Executive Officer Chris Daniels and India's IT Minister Ravi Shankar Prasad, WhatsApp agreed to work with law enforcement to develop its systems to trace the origins of 'sinister' messages.

"Facebook-owned WhatsApp assured the Indian government on Tuesday (August 21) that it would develop tools to combat the problem of fake messages, the country's information technology minister said."

"India has stepped up efforts to crack down on mass message forwards after it found that people were using platforms such as WhatsApp to stoke public anger. False messages circulated on WhatsApp have led to a series of mob beatings across the country this year."

18.08.18

Channel NewsAsia

US tech giants plan to fight India's data localisation plans

Last month the Indian main government committee on data privacy proposed a draft law placing a restriction on data flows and for all "critical personal data" to be processed within India. US tech giants such as Amazon and Microsoft attempting to push back against the draft law.

"United States technology giants plan to intensify lobbying efforts against stringent Indian data localisation requirements, which they say will undermine their growth ambitions in India, sources told Reuters."

"US trade groups, representing companies such as Amazon, American Express and Microsoft, have opposed India's push to store data locally."

23.08.18

Channel NewsAsia

Data dump: China sees surge in personal information up for sale

Despite new data protection laws being introduced in China in May, personal data has become widely available and can be bought at minimal cost by banks, insurance companies and scammers.

"When William Zhang's car insurance was about to expire in March, he didn't need to look far for renewal options. In the two months before the policy was up Zhang received calls almost daily from insurers trying to sell him a new one."

"Since his initial policy was from Ping An Insurance Group, it was natural the company had been in touch."

Internet Inclusion

21.08.18

South China Morning Post

Chinese internet users surge to 802 million in test of government's ability to manage world's biggest online community

The number of internet users in China has risen by 30 million in the first half of 2018. The total number of Chinese internet users is now over 800 million with 566 million of these using mobile payments. As the market increases so too does commercial opportunity but also the risk of illegal content.

"While two in five Chinese are still offline, the country's internet population has grown big enough to open huge market opportunities for hi-tech companies and provide the government with better access to keep watch over its citizens, according to an analyst."

"China surpassed the 800-million mark for the number of internet users for the first time, further cementing its position as home to the world's biggest online community, as the country kept up its investment in infrastructure and pushed to lower access fees."

Rest of the World

Internet governance

No new items of relevance

Cybersecurity

23.08.18

Channel NewsAsia

Australia bans China's Huawei from mobile network build over security fears

Australia has joined the US in banning major telecoms firm Huawei from supplying equipment to its 5G mobile network. The Australian Government issued a statement saying 'suppliers "who are likely to be subject to extrajudicial directions from a foreign government" would leave Australia's network vulnerable to unauthorised access or interference.

"Australia's government on Thursday (Auustg 23) banned major Chinese telecoms firm Huawei Technologies from supplying equipment for its planned 5G mobile network, citing risks of foreign interference.

Huawei's involvement in the network rollout, and resistance to it from Australia's security agencies, has become a flashpoint between the trading partners in recent months as a row over alleged Chinese meddling in Australian politics deepened."

22.08.18

Channel NewsAsia

Facebook, Twitter dismantle disinformation campaigns tied to Iran and Russia

Social media platforms have removed accounts connected to two separate propaganda campaigns, one from Iran and one from Russia. Cybersecurity firm FireEye said Iran's campaign used a network of fake news websites and fraudulent social media personas spread across social media to push narratives in line with Tehran's interests.

"Facebook Inc, Twitter Inc and Alphabet Inc collectively removed hundreds of accounts tied to an alleged Iranian propaganda operation on Tuesday, while Facebook took down a second campaign it said was linked to Russia."

"Facebook CEO Mark Zuckerberg said the accounts identified on his company's platform were part of two separate campaigns, the first from Iran with some ties to state-owned media, the second linked to sources which Washington has previously named as Russian military intelligence services."

21.08.18

Reuters

U.S. imposes fresh sanctions for Russian cyber-related activity

The U.S has imposed new sanctions on two individuals and two businesses which had attempted to help a further business circumvent previous U.S sanctions.

"The United States on Tuesday imposed sanctions on two Russians, one Russian company and one Slovakian company for what Washington said were their actions to help another Russian company avoid sanctions over the country's malicious cyber-related activities."

"The U.S. Treasury said in a statement that the sanctioned companies, Saint Petersburg-based Vela-Marine Ltd and Slovakia-based Lacno S.R.O., and the two individuals helped Divetechnoservices evade previously imposed sanctions."

Privacy

13.08.18

ABC

New tech surveillance laws more a 'side gate' than 'back door' into Australian phones

The Australian government have unveiled new surveillance laws to give law enforcement powers to access data which they were unable to do under existing legislation. The government insists that companies will not be asked to break encryption systems where they don't hold the "golden key."

"New laws will be unveiled today aimed at helping the nation's spy agencies and police monitor and prevent criminal activity through phones and the internet."

"The Federal Government reckons the current legislation is seriously out of date — it was drafted for a time when Australians would call each other on their home or office phone, and email was just a pipe dream."

Internet Inclusion

14.08.18

Reuters

Cubans cheers as internet goes nationwide for a day

The Cuban government provided a day of free internet to its citizens as it prepares to roll out the sale of internet services. President Miguel Diaz-Canel has championed the cause of boosting connectivity and will look to slowly hook homes up to the internet.

"Cuba's government said it provided free internet to the Communist-run island's more than 5 million cellphone users on Tuesday, in an eight-hour test before it launches sales of the service."

"Cuba is one of the Western Hemisphere's least connected countries. State-run telecommunications monopoly ETECSA announced the trial, with Tuesday marking the first time internet services were available nationwide."

13.08.18

Innovation Aus

Veterans reskill with cyber lessons

The Australian government has launched a programme to reskill military veterans as cybersecurity experts. The new program demonstrates how government can 'lead the way in transitioning workers into cyber and addressing the "critical" skills gap in the sector, AustCyber CEO Michelle Price said.'

"Australian military veterans will be trained as cybersecurity experts in the Department of Human Services as part of a new government program.

The federal government has partnered with employment platform WithYouWithMe to re-skill 36 navy, army and airforce veterans across three years through a 12-month contract working to protect Australia's welfare system cyber security."

22.08.18

The Daily Swig

How Africa is tackling its cybersecurity skills gap

As access to the internet grows across Africa, so too does the threat of malware and social media scams with some predicting that the African cyber skills shortage will reach 100,000 by 2020. But whilst some governments are putting in place laws that assist as opposed to deter cyber crime, such as banning tools for penetration testing, several NGOs are fostering cyber skills by holding schemes such as coding boot camps.

"Greater accessibility of mobile devices has seen digital connectivity spread throughout African countries, as the continent looks to develop its cybersecurity sector to bolster job growth and mitigate the emerging threats of online security.

Recognized African tech hubs such as those found in Kenya, South Africa, and Nigeria, have seen their communication networks transformed with Android systems, in part thanks to low-cost smartphones and greater 3G access."

15.08.18

IT News Africa

78% of African countries will offer 4G services by the end of 2018

African countries have been rapidly rolling out 4G services in the last few years. With smartphone prices decreasing and data speeds increasing, data revenues for mobile network operators look certain to increase

"A study conducted by data and analytics company, GlobalData reveals that by the end of 2018, a total of 43 out of 55 African countries (or 78%) will offer 4G services."

"In spite of this, there are a few laggards, one of them being Mozambique – a country of nearly 30 million people. However, in late July 2018, Mozambique's telecoms regulator finally announced that a 4G auction will take place in the next 2-3 months, meaning services would most likely come online in 2019. This would make Mozambique the last major economy in Southern Africa to launch 4G services."

Global Institutions

17.08.18

The Nation

Singapore calls for Asean cooperation in cybersecurity

During a meeting with Singapore's CSA, Asean nations were asked to tighten their cooperation on cybersecurity to prevent internet crime as Singapore seek to develop a rules based order for cyberspace in the region.

"During the week-long 9th Asean Journalists' Visit Programme in Singapore, 13 journalists from Asean nations were briefed by agency staff on cyber security to promote security within their own workplaces."

"CSA Deputy Chief Executive (Operations) Mr Ng Hoo Ming told the visiting group they were working with cyber security sectors in Asean by sharing experiences at the regional meeting. But some agencies had not sent enough representatives to the meeting so the CSA hoped that more agencies would participate and share lessons learnt in order to bolster cyber security in Asean."

23.08.18

Channel Life

[Cybersecurity should be priority in US $8b smart utility spend]

A digital security research firm claims that the European Commission is struggling to get its NIS Directive off the ground and obtain adequate funding for ENISA to fulfill its mandate and that most of the EU member countries have not taken the NIS directive to cyber-secure critical infrastructure seriously.

"The modernisation of utility infrastructures is enabling increased efficiencies and reliability through digitisation, connectivity, and IT-based approaches."

"Smart cyber assets are transforming both power and water grids, allowing operators to deploy and leverage a new generation of functionality and customer services."

Diary Dates

Women in Tech Council – 20.09.18

London England

5th Annual Industrial Control Cyber Security USA – 18.09.18 – 19.09.18

Sacramento, USA

ISC2 Secure Summit Toronto – 01.10.18

Toronto, Canada

MESCON Cybersecurity Conference (Middle Eastern Security Conference) Muscat – 02.10.18 – 03.10.18

Muscat, Oman