IEEE

GLOBAL INTERNET POLICY MONITOR

Read summaries of significant recent internet technology policy activities around the world

20 June 2018

Synopsis

Scroll to read full summaries with links to news articles.

The **Indian Telecommunications Regulation Authority** said **net neutrality** was a vital principle for an open internet. The Chairman of TRAI said, “it is important that the internet is kept as an open and non-discriminatory platform” and continues to be “an enabler of growth and innovation for countries like India.”

According to a new report, **China** has moved its target for launching **5G mobile technology** connections to 2019 which means it could become the first 5g-ready country in the world. The report was commissioned by multinational professional services company EY who stated that ‘China is poised to win the 5G race’ in Beijing on June 13.

Internet giant **Google** have announced that they will train up to 8,000 journalists in **India** to stop the spread of **fake news**. The hope is the network of certified trainers will then train other journalists to ‘guard journalists from falling prey to false news stories.’

The **European Parliament’s Civil Liberties Committee** has called for the **EU-US Privacy Shield**, an agreement which governs the way **United States** firms handle EU citizens data to be suspended unless the USA complies with its terms by 1st September 2018 and comes in line with the EU **General Data Protection Regulation**. This judgement comes after revelations around **Cambridge Analytica** which indicated the need for better monitoring of data protection.

A **cybersecurity** conference held in London on Monday had an all-female line up. All 15 females were experts in **cybersecurity** and the aim of the event was to encourage more women to get involved in tech related roles and to discuss the evolving threat landscape.

US President **Donald Trump** has announced that he will implement 25% tariffs on technology coming from **China** and has threatened to impose further levies if the country attempts to input retaliatory measures against the **US**.

Two Senators have introduced the **Federal Acquisition Supply Chain Security Act** which if passed would create a federal acquisition council to help stop the US Government from buying software that could be bugged with foreign spies. This Bill comes after Russian based **cybersecurity** firm **Kaspersky**, which products were used by the **United States Government**, have been accused of having links to the **Russian Government**.

The 2019 **Homeland Security Funding Bill** if passed will dramatically increase the amount the **United States** is spending on **cybersecurity**. £1.1 billion would be appropriated for cyber including $406 million for intrusion detection and prevention systems.

Educational organisation **ORT** in **South Africa** and **Chevron South Africa** have decided to collaborate to implement **coding** programmes in disadvantaged schools in north **Johannesburg** in attempt to reduce the skills gap.

Palo Alto networks, a security company based in **California,** has opened a new facility in **Sydney**. The Vice Chairman of Palo Alto Networks has pledged to reduce Australia's **cybersecurity** skills gap by helping to improve skills.

MTN SME data share, a service that gives business owners the chance to buy data bundles, has held an information session on **cybersecurity** for businesses last week in **Namibia** to discuss the importance of cybersecurity.

The head of **NATO**, General **Jens Stoltenberg** is set to encourage western allies to work together for the benefit of shared security, despite the issues between member states and the **US**. In a speech in London today he is expected to say 'the lesson of history is that we have been able to overcome our differences. Again and again, we united around our common goal. We stand together. We protect each other.'

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

20 June 2018

Table of Contents

Europe

Internet governance

***No new items of relevance*.**

Cybersecurity

13.06.18

SC Media

US sanctions Russian firms, citizens for NotPetya & other cyber-attacks

Days after US President Donald Trump urged for Russia to be part of the G7, a group consisting of the US, Canada, Italy, Japan, UK and Germany, Trump issued sanctions against five Russian companies and three citizens for being involved in the NotPetya and other cyber attacks.

"Just a few days after President Trump requested that Russia be included into the G7, the US Treasury Department issued sanctions against five Russian companies and three citizens for providing material and technical support to the Russian Federation government for the NotPetya and other cyber-attacks."

"The companies are Digital Security, ERPScan, Embedi, Kvant Scientific Research Institute and Divetechnoservices."

14.06.18

Computer Weekly

Cyber-attack warnings highlight need to be prepared

The Commander of Britain's Joint Forces Command, Christopher Deverell warned of an imminent attack on the UK control systems and other critical infrastructure. He said, 'there are many potential angles of attack on our systems' and some may come from Russia.

"Fresh warnings about the vulnerability of national infrastructure to cyber attacks show the need for securing and monitoring associated control systems connected to the internet."

"The commander of Britain's Joint Forces Command has warned that UK traffic control systems and other critical infrastructure could be targeted by cyber adversaries – but industry experts say this is nothing new and something organisations should be preparing for."

19.06.18

Computer Weekly

MPs see risk to critical infrastructure as top threat

According to a YouGov survey, more than two thirds of MPs have considered the cyber threat to national infrastructure as one of the biggest facing the UK.

"Nearly two-thirds of MPs polled consider the compromise of critical national infrastructure to be the biggest cyber threat to the UK, a YouGov survey commissioned by NCC Group has found."

"However, a year on from the cyber-attack on parliamentary emails, the survey of MPs in the House of Commons also revealed that opinion is divided about other cyber threats."

21.06.18

Forces Network

NATO Chief Appeals For Unity In Interests Of Security

The head of NATO, General Jens Stoltenberg is set to encourage western allies to work together for the benefit of shared cybersecurity, despite the issues between member states and the US. In a speech in London today he is expected to say 'the lesson of history is that we have been able to overcome our differences. Again and again, we united around our common goal. We stand together. We protect each other.'

"The head of NATO is expected to appeal to western allies to continue working together in the interests of shared security, despite a series of public differences between the US and other member states."

"In a speech in London today, NATO Secretary General Jens Stoltenberg will say that while there are real differences among alliance members, they should not be allowed to undermine the transatlantic bond."

Privacy

12.06.18

SC Media

European authorities fine Yahoo! And Optical Center

European authorities have announced that web services provider Yahoo has been fined £250,000 and Optical Center €250,000 for improperly securing their consumers data.

"European authorities have been cracking down on firm's improperly securing customer data long before GRPR went into effect with two separate companies being fined £250,000 and €250,000 respectively in the past week."

"The French Data Protection Authority (the CNIL) imposed a €250,000 fine on Optical Center for insufficiently securing personal data of its customers and the Information Commissioner's Office (ICO) issued Yahoo a £250,000 fine after an investigation into the company's 2014 breach."

13.06.18

Computer Weekly

DCMS sets out plans for National Data Strategy

The UK Department for Digital, Culture, Media and Sport have announced a new data strategy headed by Roger Taylor, co-founder of Dr Foster, a healthcare data management provider which will see a new centre for data ethics and excellence being created. The Committee have launched a consultation to seek views on the way the new centre will operate and what its priority areas of work should be.

"A new centre for data ethics and innovations will drive UK government policy making regarding data sharing and use of public data."

"The Department for Digital, Culture, Media and Sport (DCMS) has unveiled plans to boost to UK's data strategy with a new centre for data ethics and excellence, which will be headed by Roger Taylor, cofounder of Dr Foster, a provider of healthcare data management and analysis."

18.06.18

Computer Weekly

European Parliament heads for showdown with US over Privacy Shield

The European Parliament's Civil Liberties Committee has called for the EU-US Privacy Shield, an agreement which governs the way United States firms handle EU citizens data to be suspended unless the USA complies with its terms by 1st September 2018 and comes in line with the EU General Data Protection Regulation. This judgement comes after revelations around Cambridge Analytica which indicated the need for better monitoring of data protection.

"The Justice Committee of the European Parliament has set the scene for a major showdown with the US over data transfers between the EU and the US by setting a Sept 1st deadline for the US to get in compliance with EU law."

"At issue is the Privacy Shield non-legal, non-binding replacement for 'Safe Harbour", a failed agreement between the EU and the US struck down by the European Court of Justice in October 2015."

Internet Inclusion

13.06.18

Computer Weekly

Mayor Khan bids to make London the world's smartest city

The Mayor of London, Sadiq Khan has launched a new initiative to make London the world's smartest city by using smart city technology to 'solve urban challenges around air quality, city design and digital connectivity.'

"At London Tech Week, mayor Sadiq Khan launched a city-wide initiative to harness the capital's technology talent to address London's most pressing problems."

"Using digital and smart city technology to solve urban challenges around air quality, city design and digital connectivity will be the focus of a London-wide initiative launched by London mayor Sadiq Khan this week."

13.06.18

Computer Weekly

Prime minister announces new visa for startups

The UK Prime Minister Theresa May has announced plans to introduce a new startups visa for entrepreneurs in Spring 2019. The Government also promised a £2.5bn British Patient Capital Programme, which aims to help UK businesses succeed abroad and is expected to attract an additional £5bn in investment for the private sector.

"The government promises new "startup" visa for entrepreneurs, a £2.5bn British Patient Capital fund to support UK companies going global and plans for two international tech hubs."

"The government will launch a new start-up visa for entrepreneurs in spring 2019, it has promised."

18.06.18

Computer Weekly

Brexit Britain be warned, there are countries better geared to take the world's tech talent

According to the founder of a recruitment platform in Estonia, the country is better placed to attract the world's tech talent because they have introduced several policies to reduce the IT skills shortage. For example, they pioneered an e-Residency programme which gave foreigners and entrepreneurs access to Government services and was administrated to anyone with a business online.

"The founder of an Estonian recruitment platform tells Computer Weekly about how Estonia addresses its IT skills shortage."

"Estonia's immigration policy is the polar opposite of countries like the UK and US, which are trying to reduce the number of people that come from overseas to work."

18.06.18

Computer Weekly

Girls taking key stage four computing subjects down 30,000 from 2014

According to new research by the University of Roehampton the number of girls taking key stage four computing subjects was 30,000 less in 2017 compared to 2014 when it was first introduced to reduce the digital skills gap.

“The number of girls taking computing subjects at GCSE or equivalent level is significantly less than when the curriculum was introduced in 2014.”

“A study by the University of Roehampton found the number of girls taking key stage four level computing subjects was 30,000 less in 2017 than when the computing curriculum was first introduced to increase digital skills in the UK in 2014.”

18.06.18

SC Media

Reset 2018: All-female expert lineup for cybersec conference breaks mould

A cybersecurity conference held in London on Monday had an all-female line up. All 15 females were experts in cybersecurity and the aim of the event was to encourage more women to get involved in tech related roles and to discuss the evolving threat landscape.

“Reset 2018, held in central London yesterday, is a cyber-security conference with a difference, comprising insights from 15 female experts in cyber-security explaining the evolving cyber-threat landscape.”

“Joint organiser Saher Naumaan threat intelligence analyst BAE Systems commented to SC Media UK, that the event is: "Very much about cyber-security content rather than gender, so its women not simply talking about what it is like to be a woman in the industry, but about cyber-security issues.”

United States of America

Internet governance

13.06.18

Nextgov

DISA Plans to Change How Pentagon Employees Browse the Internet

The Defence Information Systems Agency have announced that they plan to alter the way in which Pentagon employees use the agencies internal networks by building a cloud system that gives employees the chance to browse the internet while removing their online footprint from the Defence Departments internal networks**.**

"The Defense Information Systems Agency doesn't want Pentagon employees using the agency's internal networks to browse the internet."

"DISA is looking for vendors to build a cloud-based system that allows employees to access the internet while isolating their online actions from the Defense Department's internal networks."

13.06.18

SC Media

US sanctions Russian firms, citizens for NotPetya & other cyber-attacks

Days after US President Donald Trump urged for Russia to be part of the G7, a group consisting of the US, Canada, Italy, Japan, UK and Germany, Trump issued sanctions against five Russian companies and three citizens for being involved in the NotPetya and other cyber attacks.

"Just a few days after President Trump requested that Russia be included into the G7, the US Treasury Department issued sanctions against five Russian companies and three citizens for providing material and technical support to the Russian Federation government for the NotPetya and other cyber-attacks."

"The companies are Digital Security, ERPScan, Embedi, Kvant Scientific Research Institute and Divetechnoservices."

15.06.18

Reuters

[Trump announces 25 percent tariff on Chinese technology]

US President Donald Trump has announced that he will implement 25% tariffs on technology coming from China and has threatened to impose further levies if the country attempts to input retaliatory measures against the US.

"President Donald Trump on Friday announced that the United States will implement a 25 percent tariff on $50 billion of goods from China related to intellectual property and technology and pledged to impose further levies if the Asian nation takes retaliatory measures."

"Trump said the tariff list includes goods from China's "Made in China 2025" strategic plan to dominate high-technology industries that will "drive future economic growth for China, but hurt economic growth for the United States and many other countries."

Cybersecurity

13.06.18

Nextgov

Trump Administration Adds to Top Cyber Ranks

The United States President Donald Trump has hired Chris Krebs, a former Microsoft Executive to be the cyber leader of the Homeland Security Department. The President has also announced his intentions to nominate Veteran Karen Evans to be the Energy Department's Assistant Secretary for cybersecurity, energy security and emergency response.

"The Trump administration strengthened its cybersecurity leadership ranks Tuesday with the confirmation of one top cyber leader at the Homeland Security Department and the appointment of another at the Energy Department."

"Chris Krebs, a former Microsoft executive who has been leading Homeland Security's cyber and infrastructure protection division in an acting capacity for several months, won Senate confirmation to officially take the role late Tuesday."

13.06.18

SC Media

US sanctions Russian firms, citizens for NotPetya & other cyber-attacks

Days after US President Donald Trump urged for Russia to be part of the G7, a group consisting of the US, Canada, Italy, Japan, UK and Germany, Trump issued sanctions against five Russian companies and three citizens for being involved in the NotPetya and other cyber attacks.

"Just a few days after President Trump requested that Russia be included into the G7, the US Treasury Department issued sanctions against five Russian companies and three citizens for providing material and technical support to the Russian Federation government for the NotPetya and other cyber-attacks."

"The companies are Digital Security, ERPScan, Embedi, Kvant Scientific Research Institute and Divetechnoservices."

13.06.18

SC media

£3.74 billion in BEC scams last year, FBI arrests 74, of which 29 Nigerian

According to data by the United States law enforcement agency the FBI, between October 2016 and December 2016 131 countries suffered from 40,203 Business Email Compromise attacks and countries lost more than £3.74 billion.

"Last year, the US FBI announced that between October 2013 and December 2016, organisations across 131 countries suffered as many as 40,203 successful Business Email Compromise (BEC) attacks, stealing £3.74 billion."

"The BEC/EAC scam continues to grow, evolve, and target small, medium, and large businesses. Between January 2015 and December 2016, there was a 2,370 percent increase in identified exposed losses. The scam has been reported in all 50 states and in 131 countries. Victim complaints filed with the IC3 and financial sources indicate fraudulent transfers have been sent to 103 countries," the premier US investigative agency noted."

18.06.18

SC Media

FBI, DHS report details new North Korean trojan

According to a new Malware Analysis Report issued by the United States, a new trojan dubbed trypeframe is being used by North Korean hacking group Hidden Cobra to send malware to unsuspecting internet users.

"Some of the positive vibes taken away from President Trump's recent meeting with North Korea's Kim Jong Un may be tempered following a joint DHS-FBI report detailing a new trojan dubbed Typeframe being used by the Hermit Kingdom."

"The Malware Analysis Report (MAR) stated Typeframe is being used by the known North Korean hacking group Hidden Cobra and federal officials are distributing the report to help reduce exposure to the malware. DHS and the FBI used 11 samples of the malware containing 32-bit and 64-bit Windows executable files and a malicious Microsoft Word document that contains Visual Basic for Applications macros."

19.06.18

Nextgov

New Bill Aims to Prevent the Next Kaspersky, ZTE

Two Senators have introduced the Federal Acquisition Supply Chain Security Bill which if passed would create a federal acquisition council to help stop the US Government from buying software that could be bugged with foreign spies. This Bill comes after Russian based cybersecurity firm Kaspersky, which products were used by the United States Government, have been accused of having links to the Russian Government.

"Federal agencies would be required to more thoroughly vet products' cybersecurity supply chains before buying them under bipartisan legislation introduced in the Senate Tuesday."

"The bill from Sens. Claire McCaskill, D-Mo., and James Lankford, R-Okla., comes six months after Congress ordered agencies to scrub the Russian anti-virus Kaspersky from their systems because of concerns it could be used by the Kremlin as a spying tool."

19.06.18

Politico

[Chinese hackers targeting satellite and defense firms, researchers find]

According to US cybersecurity firm Symantec, Chinese hackers are engaging in cyber espionage campaigns that target satellite operators, telecommunication companies and defence contractors in the US and Southeast Asia.

"Chinese hackers are waging a wide-ranging cyber espionage campaign against satellite operators, telecommunication companies and defense contractors in the U.S. and Southeast Asia, a cybersecurity company said Tuesday."

"The firm Symantec said it first noticed the campaign in January, although it has been monitoring the hacking group it dubbed "Thrip" since 2013. This year, Symantec detected "powerful malware" in Asia that it believes the hackers deployed to carry out spying operations and potentially destructive attacks."

19.06.18

Nextgov

[Senate Bill Boosts Homeland Security Cyber Funding]

The 2019 Homeland Security Funding Bill if passed will dramatically increase the amount the United States is spending on cybersecurity. £1.1 billion would be appropriated for cyber including $406 million for intrusion detection and prevention systems.

"The Homeland Security Department would receive an $86 million boost in cybersecurity money over the Trump administration's request in a funding bill forwarded by a Senate Appropriations panel Tuesday."

"The $1.1 billion cybersecurity appropriation includes $406 million for a collection of intrusion detection and prevention systems known as Einstein, according to a fact sheet."

Privacy

18.06.18

Computer Weekly

[European Parliament heads for showdown with US over Privacy Shield]

The European Parliament's Civil Liberties Committee has called for the EU-US Privacy Shield, an agreement which governs the way United States firms handle

EU citizens data to be suspended unless the USA complies with its terms by 1st September 2018 and comes in line with the EU General Data Protection Regulation. This judgement comes after revelations around Cambridge Analytica which indicated the need for better monitoring of data protection.

"The Justice Committee of the European Parliament has set the scene for a major showdown with the US over data transfers between the EU and the US by setting a Sept 1st deadline for the US to get in compliance with EU law."

"At issue is the Privacy Shield non-legal, non-binding replacement for 'Safe Harbour", a failed agreement between the EU and the US struck down by the European Court of Justice in October 2015."

Internet Inclusion

18.06.18

Nextgov

GSA Seeks Industry Feedback to Better Harness Tech Spending Data

The General Services administration, a US Government agency have announced that they wish to seek views on how to better spend the $100 billion a year they allocate to IT and digital services. Emily Murphy said, "increasing transparency on IT spending will empower federal leaders to make better informed, data-driven decisions."

"The federal government spends upwards of $100 billion on IT each year, but it wants a better understanding of how that money is being spent and is turning to industry for help."

"On Monday, the General Services Administration, in partnership with the Office of Management and Budget, released a request for information regarding "software solutions that can efficiently aggregate and analyze data across the federal enterprise."

19.06.18

Gadgets Now

Google to train 8,000 Indian journalists soon

Internet giant Google have announced that they will train up to 8,000 journalists in India to stop the spread of fake news. The hope is the network of certified trainers will then train other journalists to 'guard journalists from falling prey to false news stories.'

“New Delhi: To guard journalistsfrom falling prey to false newsstories, Google India on Tuesday said it will provide training to 8,000 journalists in English and six other Indian languages in the next one year.”

“For this, the Google News Initiative India Training Network will select 200 journalists from cities across India who will hone their skills in verification and training during five-day train-the-trainer boot camps that will be organised for English and six other Indian languages.”

Pan-Asia

Internet governance

14.06.18

Gadgets Now

Police to counter fake news on WhatsApp

Police across India have announced that they will create a social media campaign to stop the spread of fake news on sites including messaging app WhatsApp after claims such platforms had been used to incite violence.

"State police across Karnataka, Assam, Telangana and Kerala are designing social media campaigns as an antidote to fake news on messaging apps like WhatsApp following claims that these platforms have been used to incite violence across several locations in recent weeks."

"Alarmed by the rising incidence of attacks on individuals as a result of rumours spread by users of the app — owned by social network Facebook — law enforcement authorities across several states are intensifying community policing using the same platforms."

16.06.18

Gadgets Now

Trai, European telecom regulator back net neutrality

The Indian Telecommunications Regulation Authority said net neutrality was a vital principle for an open internet. The Chairman of TRAI said, "it is important that the internet is kept as an open and non-discriminatory platform" and continues to be "an enabler of growth and innovation for countries like India."

"The Telecom Regulatory Authority of India (Trai) and European telecoms regulator group BEREC have jointly backed an open internet while calling for effective regulation of electronic communications even as net neutrality rules officially expired in the US earlier this week."

"Trai and BEREC (Body of European Regulators for Electronic Communications) inked a memorandum of understanding (MoU) Thursday, underscoring their "common understanding of the building blocks of net neutrality rules" and core

aspects of the regulators' mission in preserving them, the Indian telecom regulator said in joint statement on Friday."

Cybersecurity

19.06.18

Politico

Chinese hackers targeting satellite and defense firms, researchers find

According to US cybersecurity firm Symantec, Chinese hackers are engaging in cyber espionage campaigns that target satellite operators, telecommunication companies and defence contractors in the US and Southeast Asia.

"Chinese hackers are waging a wide-ranging cyber espionage campaign against satellite operators, telecommunication companies and defense contractors in the U.S. and Southeast Asia, a cybersecurity company said Tuesday."

"The firm Symantec said it first noticed the campaign in January, although it has been monitoring the hacking group it dubbed "Thrip" since 2013. This year, Symantec detected "powerful malware" in Asia that it believes the hackers deployed to carry out spying operations and potentially destructive attacks."

20.06.18

SC Media

Israel Cyber Week: Government priorities

Israel's Prime Minister Benjamin Netanyahu has identified cybersecurity as one of the biggest threats facing the country and described it as one of the biggest businesses opportunities. 300 heads of state visited Israel to learn how the country has dealt with cyber security.

"Key to Israel's cyber-success is that Prime Minister Benjamin Netanyahu put himself in charge of cyber as he had identified it as both one of the biggest threats facing the country as well as one of its biggest business opportunities."

"At dinner in Tel Aviv with Rami Efrati, former head of the Civilian Division of the Israel National Cyber Bureau in the Prime Minister's office, and Iddo Moed, cyber coordinator at the Ministry of Foreign Affairs, SC Media UK joined international journalists for an informal briefing on the Israeli government's approach to developing a cyber-ecosystem in the country."

Privacy

No new items of relevance

Internet Inclusion

15.06.18

China Daily

EY report: China projected to win the 5G race

According to a new report, China has moved its target for launching 5G mobile technology connections to 2019 which means it could become the first 5G-ready country in the world. The report was commissioned by multinational professional services company EY who stated that 'China is poised to win the 5G race' in Beijing on June 13.

"With the global unified standard set to be finalized in the next year or so, China has moved its target timetable for the commercial launch of 5G connections to the year 2019, to potentially become one of the first 5G-ready markets in the world, according to a report released in Beijing on Wednesday."

"EY releases its report "China is poised to win the 5G race" in Beijing on June 13."

16.06.18

China Daily

5G call in Beijing a milestone for industry

On the 13th June 2018 telecommunications company Ericsson, technology company Intel and China Mobile Jiangsu Company created the first 3GPP-compliant, multi-vendor Standalone (SA) 5G New Radio (NR) call In Beijing. This marks 'another milestone in the commercialisation of the fifth generation of communication technology.'

"Swedish telecom equipment maker Ericsson, together with China Mobile Research Institute and US tech giant Intel, completed on Friday a 3GPP-compliant, multivendor Standalone 5G New Radio (NR) call in Beijing, marking another milestone in the commercialization of the fifth generation of communication technology."

"The move is also the first multivendor 5G call to meet 3GPP's standalone 5G NR specifications, right after the global mobile industry completed the world's 5G standard by approving technical specifics for the standalone network of 5G."

19.06.18

Gadgets Now

Google to train 8,000 Indian journalists soon

Internet giant Google have announced that they will train up to 8,000 journalists in India to stop the spread of fake news. The hope is the network of certified trainers will then train other journalists to 'guard journalists from falling prey to false news stories.'

"New Delhi: To guard journalistsfrom falling prey to false newsstories, Google India on Tuesday said it will provide training to 8,000 journalists in English and six other Indian languages in the next one year."

"For this, the Google News Initiative India Training Network will select 200 journalists from cities across India who will hone their skills in verification and training during five-day train-the-trainer boot camps that will be organised for English and six other Indian languages."

20.06.18

Gadgets Now

Only 25% adults use Internet in India: Pew survey

According to a new survey by Pew Research Center, only 25% of adults in India reportedly used the internet in 2017. In contrast 96% of adults used the internet in South Korea in that same year.

"Despite talk of Digital India, only one-in-four in the country reported using the Internet in 2017, which is among the lowest in the world, according to a new survey by the Pew Research Center."

"South Korea stands out as the most heavily connected society, with 96 per cent of adults reporting Internet use, showed the survey conducted in 37 countries."

Rest of the World

Internet governance

No new items of relevance

Cybersecurity

13.06.18

SC Media

US sanctions Russian firms, citizens for NotPetya & other cyber-attacks

Days after US President Donald Trump urged for Russia to be part of the G7, a group consisting of the US, Canada, Italy, Japan, UK and Germany, Trump issued sanctions against five Russian companies and three citizens for being involved in the NotPetya and other cyber attacks.

"Just a few days after President Trump requested that Russia be included into the G7, the US Treasury Department issued sanctions against five Russian companies and three citizens for providing material and technical support to the Russian Federation government for the NotPetya and other cyber-attacks."

"The companies are Digital Security, ERPScan, Embedi, Kvant Scientific Research Institute and Divetechnoservices."

14.06.18

Computer Weekly

Cyber-attack warnings highlight need to be prepared

The Commander of Britain's Joint Forces Command, Christopher Deverell warned of an imminent attack on the UK control systems and other critical infrastructure. He said, 'there are many potential angles of attack on our systems' and some may come from Russia.

"Fresh warnings about the vulnerability of national infrastructure to cyber attacks show the need for securing and monitoring associated control systems connected to the internet."

"The commander of Britain's Joint Forces Command has warned that UK traffic control systems and other critical infrastructure could be targeted by cyber adversaries – but industry experts say this is nothing new and something organisations should be preparing for."

17.06.18

The Hill

Spotlight falls on Russian threat to undersea cables

The US President Donald Trump has introduced new sanctions on Russia because of the threats they pose to undersea cables that carry the world's electronic communications between continents.

"The Trump administration's new sanctions on Russia are casting light on the threat posed to the undersea cables that carry the world's electronic communications between continents."

"The Treasury Department sanctioned five Russian firms and three Russian nationals this week for aiding the Kremlin's domestic security service, the FSB. One of the companies is alleged to have provided support for Moscow's "underwater capabilities" — including producing diving systems and a submersible craft for the FSB."

18.06.18

SC Media

FBI, DHS report details new North Korean trojan

According to a new Malware Analysis Report issued by the United States a new trojan dubbed trypeframe is being used by North Korean hacking group Hidden Cobra to send malware to unsuspecting internet users.

"Some of the positive vibes taken away from President Trump's recent meeting with North Korea's Kim Jong Un may be tempered following a joint DHS-FBI report detailing a new trojan dubbed Typeframe being used by the Hermit Kingdom."

"The Malware Analysis Report (MAR) stated Typeframe is being used by the known North Korean hacking group Hidden Cobra and federal officials are distributing the report to help reduce exposure to the malware. DHS and the FBI used 11 samples of the malware containing 32-bit and 64-bit Windows executable files and a malicious Microsoft Word document that contains Visual Basic for Applications macros."

19.06.18

Nextgov

New Bill Aims to Prevent the Next Kaspersky, ZTE

Two Senators have introduced the Federal Acquisition Supply Chain Security Bill which if passed would create a federal acquisition council to help stop the US Government from buying software that could be bugged with foreign spies. This Bill comes after Russian based cybersecurity firm Kaspersky, which products were used by the United States Government, have been accused of having links to the Russian Government.

"Federal agencies would be required to more thoroughly vet products' cybersecurity supply chains before buying them under bipartisan legislation introduced in the Senate Tuesday."

"The bill from Sens. Claire McCaskill, D-Mo., and James Lankford, R-Okla., comes six months after Congress ordered agencies to scrub the Russian anti-virus Kaspersky from their systems because of concerns it could be used by the Kremlin as a spying tool."

Privacy

No new items of relevance

Internet Inclusion

13.06.18

IT News Africa

WeThinkCode_ trains young developers at no cost

WeThinkCode which was co-founded by Arlene Mulder and Camille Agon has sought to revolutionise the educational system by developing digital talent and teaching essential transferrable skills in Africa.

"From before the invention of the QWERTY keyboard in 1868 and up to the ongoing advancements in Artificial Intelligence (AI) today, individuals have explored and redefined the boundaries of what was previously deemed possible – and it is safe to assume that we have only seen the tip of the iceberg."

"Technology has the power to be the biggest catalyst for change in the educational sector, wielding the potential for genuine transformation. Gaynor MacArthur, Director of Sales at Apple Premium Reseller, Digicape, says that one

of the most rewarding aspects of her role is being able to support and work alongside other businesses with values that mirror Digicape's own."

14.06.18

Namibia Economist

MTN SME Masterclass Zooms In On Cybersecurity

MTN SME, data share, a service that gives business owners the chance to buy data bundles, has held an information session on cybersecurity for businesses last week in Namibia to discuss the importance of cybersecurity.

"MTN SME Masterclass held an information session on cybersecurity for businesses last week at the Safari Court Hotel."

"Speakers at the event agreed that there is an increased opportunity for local businesses with a computer or mobile device and a reliable internet connection to participate in the global digital economy."

16.06.18

IT News Africa

Creating coding prodigies in previously disadvantaged schools

Educational organisation ORT in South Africa and Chevron South Africa have decide to collaborate to implement coding programmes in disadvantaged schools in north Johannesburg in an attempt to reduce the skills gap.

"Learning to code is a critical element in the 21st century school curriculum, giving learners the ability not only to use technology but to create it, as the world ushers in the fourth industrial revolution. Learners equipped with these skills will be in high demand in the labour market of the future."

"Non-profit educational organization, ORT South Africa (ORT SA) and Chevron South Africa have partnered up to implement coding programmes in previously disadvantaged schools in Ivory Park, north of Johannesburg."

19.06.18

Security Brief Asia

Palo Alto Networks extends Cyber Range reach through first APAC facility

Palo Alto networks a security company based in California has opened a new facility in Sydney. The Vice Chairman of Palo Alto Networks has pledged to reduce Australia's cybersecurity skills gap by helping to improve skills.

"Palo Alto Networks has opened the doors to its newest facility that joins its global Cyber Range initiative."

*"The Sydney Cyber Range is now the company's first Asia Pacific Cyber Range facility, and the fourth permanent facility worldwide**."***

20.06.18

The Guardian

Experts want women to bridge digital gap, leverage tech for jobs

Experts from a technology forum in Lagos have urged women to get more involved in information communications technology related jobs. Carole Wanjau, Responsibility leader, African and Middle East, Commins said, 'we are in a digital age, women should take up technical and digital jobs instead of leaving them for their male- counterparts.'

"Experts have urged women to leverage the digital space for information communications technology (ICT) jobs."

"The call was made at a technology forum in Lagos, with the aim of empowering Nigerian women to optimise their innate potential and develop capabilities to achieve success through collaboration and empowerment."

Global Institutions

21.06.18

Forces Network

NATO Chief Appeals For Unity In Interests Of Security

The head of NATO, General Jens Stoltenberg is set to encourage western allies to work together for the benefit of shared cybersecurity, despite the issues between member states and the US. In a speech in London today he is expected to say ‘the lesson of history is that we have been able to overcome our differences. Again and again, we united around our common goal. We stand together. We protect each other.’

“The head of NATO is expected to appeal to western allies to continue working together in the interests of shared security, despite a series of public differences between the US and other member states.”

“In a speech in London today, NATO Secretary General Jens Stoltenberg will say that while there are real differences among alliance members, they should not be allowed to undermine the transatlantic bond.”

Diary Dates

M-Trends 2018: The Trends Behind Today's Breaches and Cyber Attacks – 21.06.18

London, England

Data Centre Risk Radar – Technical Skills Shortage – 27.06.18

London, England

CyberFirst Briefing with NCSC – 11.07.18

London, England

Women in Tech Council – 20.09.18

London England