30 May 2018

Synopsis

Scroll to read full summaries with links to news articles.

China has announced that more than $17.2 billion will be allocated by 2020 to reform their manufacturing sector with **new technologies** and for **higher education**, creating 137 universities to produce quality talent that can turn China into a technology powerhouse by 2035.

According the **Chen Yin**, the Chief Engineer at China's top industry regulator the **Ministry of Industry and Information Technology** announced that **China** will speed up their three-year plan to boost industrial **cybersecurity** as it becomes more of a high priority for the country.

The **Chinese Government** has announced they will focus more effort on promoting and creating domestic chips for Government agencies and state-owned enterprises. This will put pressure on US technology firm **Intel Corp**, whose main market is China.

Four **EU** cybersecurity organisations, the European Union Agency for Network and Information Security (**ENISA**), the European Defence Agency (**EDA**), **Europol** and the Computer Emergency Response Team for the EU Institutions, Agencies and Bodies (**CERT-EU**) have signed a memorandum of understanding to cooperate on all things **cybersecurity** related to avoid duplication of effort.

Speaking at a technology conference with US technology giants such as **Microsoft**, French President **Emmanuel Macron** said **Europe** should create global standards for tougher regulation of the **digital technology**. These rules should be somewhere in between the US model which is not sufficiently strict and the Chinese model which is too restrictive.

In a **Ministry of Defence** report on **Artificial Intelligence**, it was suggested that robots which train themselves in battle tactics by playing **video games** could be used to mount **cyber attacks**. Researchers in Silicon Valley are using strategy games, such as StarCraft II, to teach systems how to solve complex problems on their own. These Artificial Intelligence programs can then "be readily adapted" to wage **cyberwarfare**, the MoD says.

The **Senate Armed Services Committee** have attempted to create a new **cyber warfare** strategy by passing a version of the **Defence Policy Bill** even though US President **Donald Trump** passed his own classified strategy to Congress in April. If this becomes law, it would mean the **United States** would use 'all instruments of national power' including military and offensive force and digital operations to deal with large scale cyber attacks.

Internet giant Facebook's Chief Executive has apologised to the **European Parliament** for not effectively dealing with **fake news** and for being involved in a major data scandal which saw political consultancy firm **Cambridge Analytica** use the data of thousands of **Facebook** users to influence the **US Presidential elections** and the **UK Brexit vote**.

The **US** federal agencies have been barred from using **cybersecurity software** made by **Russian** based security software company, **Kaspersky**, over fears the firm has ties to the Russian Government's spying programs. However, the agencies have been struggling to remove it because Congress have provided no funding to replace these devices.

Kenya's new **Computer Misuse and Cybercrimes Act** which became law on the 16th May 2018 have raised concerns that it restricts freedom of expression and access to information. This is because the new act criminalises **hate speech** and false publications however there is no definition to distinguish what constitutes as hate speech from speech that Is protected under Kenya's existing laws.

Russia has urged American technology company **Apple** to remove **Telegram** from the app store after the messaging app refused to provide the Russian Government with access to their **user's data.**

Olurotimi Akeredolu, the Governor of Ondo State in **Nigeria**, has announced a new **digital resource center** which will be used to help improve the education and learning delivery in schools.

The **European Internet Service Providers Association** and the IT security and performance firm **Cloudflare** Another have become the two latest members to join the **Council of Europe's** cooperation agreement to promote an open and safe **internet**. They join eight other technology firms including Apple, Facebook, Google, Microsoft, Kaspersky Lab and Orange and Telefónica.

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

30 May 2018

Table of Contents

Synopsis 1

Europe 4
- Internet governance 4
- Cybersecurity 4
- Privacy 7
- Internet Inclusion 9

United States of America 12
- Internet governance 12
- Cybersecurity 12
- Privacy 15
- Internet Inclusion 16

Pan-Asia 17
- Internet governance 17
- Cybersecurity 17
- Privacy 18
- Internet Inclusion 18

Rest of the World 22
- Internet governance 22
- Cybersecurity 22
- Privacy 24
- Internet Inclusion 25

Global Institutions 29

Diary Dates 30

Europe

Internet governance

24.05.18

Channel NewsAsia

Wary of China, Macron urges Europe to set tech regulation standards

Speaking at a technology conference with US technology giants such as Microsoft, French President Emmanuel Macron said Europe should create global standards for tougher regulation of the digital technology. He said, these rules should be somewhere in-between the US model which is not sufficiently strict and the Chinese model which is too restrictive.

"Europe should set global standards for tougher regulation of digital technology, finding a way between an excessively lax United States and an over-restrictive China, French President Emmanuel Macron said on Thursday."

"Addressing the bosses of U.S. giants Microsoft and IBM at a Paris technology conference, Macron said the European Union's new data privacy regulation, known as GDPR, demonstrated Europe's ability (EU) to lead the way."

Cybersecurity

23.05.18

Ministry of Defence

Human-Machine Teaming

In a Ministry of Defence report on Artificial Intelligence, it was suggested that robots which train themselves in battle tactics by playing video games could be used to mount cyber attacks. Researchers in Silicon Valley are using strategy games, such as StarCraft II, to teach systems how to solve complex problems on their own. These Artificial Intelligence programs can then "be readily adapted" to wage cyberwarfare, the MoD says.

"Throughout history, new technologies have been a driver of military adaptation and advantage."

"Whether moving from sail to steam, horses to tanks, or the introduction and exploitation of the aeroplane or radio, the results have often been transformative.

When it has been transformative, strategy, tactics and technology have often evolved symbiotically; invariably when people figure out how best to exploit the full potential of the emerging combination of technologies."

23.05.18

GOV.UK

Cyber and International Law in the 21st Century

The Attorney General Jeremy Wright explained the UK's position on international cyber-space law. He said it should never be a lawless world and those states and individuals that engage in hostile cyber operations should be governed by the law just like in any other area on earth.

"The Attorney General Jeremy Wright QC MP this morning set out the UK's position on applying international law to cyberspace. This is the first time a Government Minister has set out the UK view on record."

"I am particularly pleased to be speaking here, at Chatham House Royal Institute for International affairs, which has a longstanding record of engaging governments, the private sector and civil society in debate about the most significant and pressing developments in international affairs."

24.05.18

Security Brief Asia

BMW awards Chinese security team's work in exposing connected vehicle vulnerabilities

Tencent Keen Security Lab, a security company based in China have been rewarded by German carmaker BMW after finding and fixing several vulnerabilities in their connected vehicles which could have been remotely hacked by cyber criminals.

"When Chinese security researchers found a number of vulnerabilities in BMW's connected vehicles, BMW didn't just fix the vulnerabilities, it even awarded the eagle-eyed researchers for their efforts."

"Tencent Keen Security Lab examined BMW's internet connected systems (Infotainment System (a.k.a Head Unit), Telematics Control Unit and Central Gateway Module) and found that an attacker could potentially conduct a remote targeted attack on multiple vehicles."

28.05.18

New Europe

TDL /NE event sheds light on future of EU cybersecurity assessments.

Trust in Digital Life, a membership association for leading industry partners within the EU and newswire, New Europe, held a roundtable last week which saw leading experts discuss the EU Cybersecurity Act and how to create a 'safer computing ecosystem' for the public.

"On May 24, Trust in Digital Life and New Europe co-hosted a half-day roundtable event at the Press Club Brussels, which brought together representatives from the European Institutions, academia and industry to discuss issues surrounding the security assessment area."

"The EU Cybersecurity Act, currently under discussion at the European Parliament and the Council of the EU, is generating considerable debate on risk analysis, best practices, certification frameworks, self-assessment techniques, and other challenges the EU needs to address to create a safer computing ecosystem for its citizens."

30.05.18

The Times

Outdated IT hampering fight against cybercrime, say Police Scotland

The UK Police in Scotland have asked the Government to provide them with more than £200 million to update their outdated IT equipment which they claim is hampering their ability to fight against cybercrime.

"Police chiefs have admitted that dated IT equipment has left them struggling to tackle cybercrime in Scotland and are to demand more than £200 million for new technology."

"The urgent cash injection is needed to finally deliver an integrated system capable of recording and analysing information across the country and to pay for advanced tools, which officers believe will make them more efficient."

Privacy

23.05.18

Channel NewsAsia

['I'm sorry', Facebook's Zuckerberg tells European lawmakers](#)

Internet giant Facebook's Chief Executive has apologised to the European Parliament for not effectively dealing with fake news and for being involved in a major data scandal which saw political consultancy firm Cambridge Analytica use the data of thousands of Facebook users to influence the U.S. Presidential elections and the Brexit vote.

"Facebook chief Mark Zuckerberg apologised to the European Parliament on Tuesday (May 22) for the "harm" caused by a huge breach of users' data and by a failure to crack down on fake news."

"But Zuckerberg's appearance failed to satisfy MEPs who accused him of dodging questions and criticised a format that gave the parliament's political leaders far more time to give long-winded speeches."

24.05.18

SC Media

Four EU cyber-security organisations enhance cooperation, avoid duplication

Four EU cyber security organisations, the European Union Agency for Network and Information Security (ENISA), the European Defence Agency (EDA), Europol and the Computer Emergency Response Team for the EU Institutions, Agencies and Bodies (CERT-EU) have signed a memorandum of understanding to cooperate on all things cybersecurity related to avoid duplication of effort.

"Yesterday (Wednesday 23 May) ENISA, EDA, Europol and the CERT-EU signed a Memorandum of Understanding (MoU) to establish a cooperation framework between their organisations."

"The European Union Agency for Network and Information Security (ENISA), the European Defence Agency (EDA), Europol and the Computer Emergency Response Team for the EU Institutions, Agencies and Bodies (CERT-EU) signed a Memorandum of Understanding (MoU) to establish a cooperation framework between their organisations on Wednesday 23 May."

25.05.18

Channel NewsAsia

EU privacy law enters into force, activist takes aim

Privacy activists have already taken action against US tech firms who are failing to comply with privacy laws introduced on the 25th May 2018 which makes companies obliged to think about how they handle personal data. Australian Lawyer Max Shrems explained that US Tech giants are illegally forcing users to consent to new privacy policies which is 'totally against the law.'

"New European privacy regulations went into effect on Friday that will force companies to be more attentive to how they handle customer data."

"The ramifications were visible from day one, with major U.S.-media outlets including the LA Times and Chicago Tribune were forced to shutter their websites in parts of Europe."

26.05.18

Channel NewsAsia

Heightened debate in US as EU privacy rules take effect

Nearly all US tech firms are subjected to new strict EU privacy laws which regulate how firms handle data because a large majority of them have online operations in the European Union. This has caused a debate on privacy laws in the United States with some calling for similar rules and others claiming it could 'fracture the whole internet.'

"Amid a global scramble to comply with new EU data protections laws, the debate on privacy has intensified in the United States with some calling for similar measures for Americans, and others warning the rules could fracture the global internet."

"US tech firms, and virtually all companies with online operations, will need to comply with the rules if their sites are used in the European Union, or face hefty financial penalties."

Internet Inclusion

23.05.18

Council of Europe

Council of Europe co-operation with IT sector: two new partners

The European Internet Service Providers Association and the IT security and performance firm Cloudflare Another, have become the two latest members to join the Council of Europe's cooperation agreement to promote an open and safe internet. They join eight other technology firms including Apple, Facebook, Google, Microsoft, Kaspersky Lab and Orange and Telefónica.

"The Council of Europe´s Secretary General, Thorbjørn Jagland, today signed collaboration agreements - in the form of an exchange of letters – with the European Internet Service Providers Association (EuroISPA) and the IT security and performance firm Cloudflare to promote respect for human rights, democracy and the rule of law online."

"These new partners join another eight technology firms and six associations which entered into the same kind of co-operation agreement with the Council of Europe in November 2017."

24.05.18

Police and Crime Commissioner

Young super sleuths encouraged to enter cyber challenge

A new cyber security challenge funded by West Yorkshire Police's Proceeds of Crime Act fund, which takes money away from criminals and reinvests it back into the community, are encouraging young adults aged 11-17 to enter the first-ever Matrix 2018 challenge. This is an online cyber competition from which the top 64 participants will go forward to a live final event.

"Super sleuths aged from 11 to 17 are being encouraged to enter the first-ever Matrix 2018 challenge which will focus on an online cyber / competition themed challenge from which the top 64 participants will go forward to a live final event."

"The challenge has been funded by West Yorkshire Police's Proceeds of Crime Act (POCA) fund which takes money away from criminals and reinvests it back into the community. It is being delivered by the Yorkshire and Humber Regional Cyber Crime Unit."

28.05.18

Channel NewsAsia

[France, Germany push for EU funding for technology start-ups]

France and Germany have urged for more EU funding for innovation and research into technology start-ups, so Europe can lead the way in technological development ahead of China and the United States.

"France and Germany are pushing for an EU-wide initiative to fund innovation and research in tech start-up projects across the bloc so that Europe can compete more effectively against the likes of China and the United States."

"Europe has long been seen as a laggard in developing new technologies compared with the United States, which has a strong venture capital industry funding Silicon Valley start-ups."

25.05.18

Channel NewsAsia

[Britain will build own satellite system if no access to EU's: Hammond]

According to Britain's Finance Minister Philip Hammond announced that the UK will create its own satellite navigation system if Europe stops the UK from accessing the Galileo project, their version of GPS.

"Britain would develop its own separate satellite navigation system if it lost access to the Galileo project, the European Union's version of GPS, Britain's finance minister said on Friday."

"Britain told the European Union on Thursday it will demand the repayment of up to 1 billion pounds (US$1.34 billion) if the bloc restricts its access to Galileo."

29.05.18

Computer Weekly

[Drone industry set to contribute £42bn to UK economy by 2030]

According to new research by PWC a multinational services network drone technology could add £42 billion to the UK economy by 2030 and create more than 68,000 jobs.

"PwC research has predicted drones could add £42bn to the economy and create 68,000 jobs by 2030."

“Enterprise adoption of drone technologies could add £42bn to the UK GDP by 2030 through automating repetitive workplace processes, enabling staff to focus on higher-value work, according to a report by business advisory firm, PwC.”

28.05.18

China Daily

China, EU essential partners to each other's AI strategy

According to the President of ChinaEU, Luigi Gambardella a digital association based in Brussels said China is ‘essential for Europe’s AI strategy, and vice versa.’ She urged both countries to work together in technology because Europe is less digitalised so ‘China will be an appealing and promising market for the EU’s future AI companies.’

“China is unique and essential for Europe's AI strategy, and vice versa, said a European business leader.”

"It is beneficial for both sides to jointly work on this topic, and this is the right time for Brussels and Beijing to deepen their cooperation," Luigi Gambardella, president of ChinaEU, a business-led international digital association in Brussels, told Xinhua in a recent interview.”

30.05.18

Computer Weekly

Firms step up spending on digital tech, but struggle with strategy

According to research by consulting and audits firm Deloitte, Businesses in the UK are spending more on technologies including, blockchain and artificial intelligence, however, most executives do not feel comfortable to develop a coherent strategy to lead their companies through digital change.

“Businesses and the public sector are stepping up their spending on digital technology, but many business leaders are struggling to keep pace with what it means for their business.”

“Organisations have stepped up their spending on cutting-edge technologies, including artificial intelligence, blockchain and virtual reality, over the past 12 months, but many are struggling to develop a coherent strategy for their investment plans, according to research by Deloitte.”

United States of America

Internet governance

No new items of relevance

Cybersecurity

23.05.18

The Hill

Federal agencies struggle to get Kaspersky software off their systems: report

The US federal agencies have been barred from using cybersecurity software made by Russian based security software company, Kaspersky, over fears the firm has ties to the Russian Government's spying programs. However, the agencies have been struggling to remove it because Congress have provided no funding to replace these devices.

"Federal agencies are having a hard time getting Kaspersky Labs software off their computers after Congress passed legislation mandating that they do so, reports the Daily Beast."

"The National Defense Authorization Act (NDAA) passed by Congress last November requires agencies to stop using products created by Kaspersky Labs, a Russian security software company."

25.05.18

The Hill

FBI issues formal warning on massive malware network linked to Russia

The United States Federal Bureau of Investigation said a sophisticated Russian hacking campaign have infiltrated thousands of home networks and home offices with a VPNFilter. The FBI have advised home users to reboot their devices.

"The FBI on Friday issued a formal warning that a sophisticated Russia-linked hacking campaign is compromising hundreds of thousands of home network devices worldwide and it is advising owners to reboot these devices in an attempt to disrupt the malicious software."

"The law enforcement agency said foreign cyber actors are targeting routers in small or home offices with a botnet — or a network of infected devices — known as VPNFilter."

25.05.18

The Hill

Senate panel again looks to force Trump's hand on cyber warfare strategy

The Senate Armed Services Committee have attempted to create a new cyber warfare strategy by passing a version of the Defence Policy Bill even though US President Donald Trump passed his own classified strategy to Congress in April. If this becomes law, it would mean the United States would use 'all instruments of national power' including military and offensive force and digital operations to deal with large scale cyber attacks.

"A Senate panel is attempting again to dictate a cyber policy strategy — even after the Trump administration submitted its own, classified strategy to Congress last month."

"The Senate Armed Services Committee on Thursday approved a new version of the annual defense policy bill, formally known as the National Defense Authorization Act (NDAA), 25-2."

28.05.18

Security Brief Asia

Trump cancelling North Korea summit will have 'cyber-retaliation'

It has been warned that if the US President Donald Trump cancels the meeting with North Korean leader Kim Jong Un then the US will suffer from a 'cyber-retaliation.'

"Headlines around the world have been painted with the news that Trump has cancelled a historic US-North Korea summit – which could have huge implications on the US's cybersecurity."

"It would have been the first time a sitting US president met a North Korean leader, but it seems not to be after North Korea released statements belittling US vice president Mike Pence."

29.05.18

Channel NewsAsia

Cyber thieves claim to hit two big Canadian banks

The Bank of Montreal and Canadian Imperial Bank of Commerce have announced that a cyber-attack on their platforms could have led to hackers gaining access to tens of thousands of customers data.

"Bank of Montreal and Canadian Imperial Bank of Commerce said on Monday that cyber attackers may have stolen the data of potentially tens of thousands of customers in what could be the first significant assault on financial institutions in the country."

"Bank of Montreal, Canada's fourth biggest lender, said on Monday it was contacted by fraudsters on Sunday who claimed they were in possession of the personal and financial information of a limited number of the bank's customers."

30.05.18

Reuters

US warns again on hacks it blames on North Korea

The US Department of Homeland Security have issued their third warning and published technical details over a number of attacks which happened back in 2009 by the group "Hidden Cobra" which they have blamed on North Korea.

"The U.S. government on Tuesday released an alert with technical details about a series of cyber attacks it blamed on the North Korean government that stretch back to at least 2009."

"The warning is the latest from the Department of Homeland Security and the Federal Bureau of Investigation about hacks that the United States charges were launched by the North Korean government."

Privacy

23.05.18

Channel NewsAsia

'I'm sorry', Facebook's Zuckerberg tells European lawmakers

Internet giant Facebook's Chief Executive has apologised to the European Parliament for not effectively dealing with fake news and for being involved in a major data scandal which saw political consultancy firm Cambridge Analytica use the data of thousands of Facebook users to influence the US Presidential elections and the Brexit vote.

"Facebook chief Mark Zuckerberg apologised to the European Parliament on Tuesday (May 22) for the "harm" caused by a huge breach of users' data and by a failure to crack down on fake news."

"But Zuckerberg's appearance failed to satisfy MEPs who accused him of dodging questions and criticised a format that gave the parliament's political leaders far more time to give long-winded speeches."

25.05.18

Channel NewsAsia

Facebook launches searchable archive of US political ads

Internet giant Facebook have launched a new archive which shows who has paid for political ads in the United States after public outcry that Russia purchased ads to influence the 2016 Presidential election. The feature will be rolled out to other countries in a few months.

"Facebook Inc. on Thursday launched an archive of U.S. political ads that appear on the world's largest social network, showing who paid for them and other details, after an outcry over Russians' alleged purchase of such ads during the 2016 elections."

"The archive tool will be rolled out to other countries in coming months, it added."

Internet Inclusion

24.05.18

China Daily

Domestic chips to get a big boost

The Chinese Government have announced they will focus more effort on promoting and creating domestic chips for Government agencies and state-owned enterprises. This will put pressure on US technology firm Intel Corp, whose main market is China.

"Government procurement in China to include homegrown processors."

"China is including domestic processors in its government procurement plans, as the nation steps up its effort to promote the application of homegrown chips in government agencies and State-owned enterprises."

29.05.18

The Hill

Russia asks Apple to ban messaging app Telegram

Russia have urged American technology company Apple to remove Telegram from their app store after the messaging app refused to provide the Russian Government with access to their user's data**.**

"Russia is asking Apple to remove Telegram from its app store after the messaging app refused requests to give the government backdoor access to its platform."

"Russia had tried to ban Telegram earlier this year but is reportedly having a difficult time completely blocking the app within its borders."

Pan-Asia

Internet governance

No new items of relevance

Cybersecurity

24.05.18

Security Brief Asia

BMW awards Chinese security team's work in exposing connected vehicle vulnerabilities

Tencent Keen Security Lab, a security company based in China have been rewarded by German carmaker BMW after finding and fixing several vulnerabilities in their connected vehicles which could have been remotely hacked by cyber criminals.

"When Chinese security researchers found a number of vulnerabilities in BMW's connected vehicles, BMW didn't just fix the vulnerabilities, it even awarded the eagle-eyed researchers for their efforts."

"Tencent Keen Security Lab examined BMW's internet connected systems (Infotainment System (a.k.a Head Unit), Telematics Control Unit and Central Gateway Module) and found that an attacker could potentially conduct a remote targeted attack on multiple vehicles."

25.05.18

ChinaDaily

Industrial cybersecurity a 'high priority'

According the Chen Yin, the Chief Engineer at China's top industry regulator the Ministry of Industry and Information Technology announced that China will speed up their three-year plan to boost industrial cybersecurity as it becomes more of a high priority for the country.

“China will speed up the implementation of a three-year plan to boost industrial cybersecurity, as the convergence of cutting-edge information technology and industry gathers momentum in the nation.”

“Chen Yin, chief engineer of the Ministry of Industry and Information Technology, China's top industry regulator, said on Thursday that ensuring cybersecurity should be a high priority as companies are scrambling to promote the development of the industrial internet.”

Privacy

No new items of relevance

Internet Inclusion

23.04.18

China Daily

'Robo-adviser' research lab established

A new 5 million-yuan Robo-adviser lab has been established in China by Tonji University and Shanghai an internet finance information company. The lab will focus on four research areas including offering talent training and business advice to companies.

“A ‘robo-advisers’ lab was established jointly by Tongji University and an internet finance information company in Shanghai on Wednesday, the first of its kind in China.”

“Co-founded by the technological management institute at Tongji University and internet finance information service company Yushi, the lab received 5 million yuan ($783,219) as its initial investment.”

24.05.18

China Daily

Domestic chips to get a big boost

The Chinese Government have announced they will focus more effort on promoting and creating domestic chips for Government agencies and state-owned enterprises. This will put pressure on US technology firm Intel Corp, whose main market is China.

"Government procurement in China to include homegrown processors."

"China is including domestic processors in its government procurement plans, as the nation steps up its effort to promote the application of homegrown chips in government agencies and State-owned enterprises."

28.05.18

China Daily

China, EU essential partners to each other's AI strategy

According to the president of ChinaEU, Luigi Gambardella a digital association based in Brussels said China is 'essential for Europe's AI strategy, and vice versa.' She urged both countries to work together in technology because Europe is less digitalised so 'China will be an appealing and promising market for the EU's future AI companies.'

"China is unique and essential for Europe's AI strategy, and vice versa, said a European business leader."

"It is beneficial for both sides to jointly work on this topic, and this is the right time for Brussels and Beijing to deepen their cooperation," Luigi Gambardella, president of ChinaEU, a business-led international digital association in Brussels, told Xinhua in a recent interview."

28.05.18

China Daily

China, India launch IT industry cluster to boost cooperation

Guiyang the capital of Guizhou Province in Southwest China has joined with Indian IT industry association and an Indian educational learning enterprise to increase cooperation between the two countries to help develop their digital economies.

“A China-India IT industry cluster was launched Sunday in Southwest China's Guizhou province, in a bid to step up cooperation between the two countries through integrated development.”

“Guiyang, capital of Guizhou, has joined hands with NASSCOM, an Indian non-profit IT industry association, and NIIT, an Indian talent development enterprise, to launch a series of cooperation projects.”

28.05.18

China Daily

Big money aimed at top universities

China have announced that more than $17.2 billion will be allocated by 2020 to reform their manufacturing sector with new technologies and invest it in higher education, creating 137 universities to produce quality talent that can turn China into a technology powerhouse by 2035.

“China will devote more resources to reforming its manufacturing sector with new, innovative technologies, while improving the higher education system's ability to produce quality talent capable of original, groundbreaking work, officials said on Saturday.”

“China will invest around 110 billion yuan ($17.2 billion) by 2020 to help the country's top 42 universities become first-class institutions, while creating 137 universities with first-class standing in specific fields, Yang Wei, former director of the National Natural Science Foundation of China, said during a panel discussion at the 20th annual meeting of the China Association of Science and Technology in Hangzhou, Zhejiang province, which opened on Saturday.”

29.05.18

China Daily

Deals worth over 35b yuan signed at big data expo

During the China International Big Data Industry Expo in Guiyang which is in Southwest China more than 199 deals worth more than 35 billion yuan were signed and more than 65 forums held discussions on artificial intelligence and the Internet of Things.

“A total of 199 deals worth more than 35 billion yuan ($5.4 billion) were signed during the China International Big Data Industry Expo in Guiyang, capital of Southwest China's Guizhou province.”

“Eight panel discussions and 65 forums focusing on artificial intelligence (AI), data security, Internet of Things, shared economy, and targeted poverty alleviation were held during the expo that started on Saturday.”

Rest of the World

Internet governance

No new items of relevance

Cybersecurity

23.05.18

The Hill

Federal agencies struggle to get Kaspersky software off their systems: report

The US federal agencies have been barred from using cybersecurity software made by Russian based security software company, Kaspersky, over fears the firm has ties to the Russian Government's spying programs. However, the agencies have been struggling to remove it because Congress have provided no funding to replace these devices.

"Federal agencies are having a hard time getting Kaspersky Labs software off their computers after Congress passed legislation mandating that they do so, reports the Daily Beast."

"The National Defense Authorization Act (NDAA) passed by Congress last November requires agencies to stop using products created by Kaspersky Labs, a Russian security software company."

25.05.18

The Hill

FBI issues formal warning on massive malware network linked to Russia

The United States Federal Bureau of Investigation said a sophisticated Russian hacking campaign have infiltrated thousands of home networks and home offices with a VPNFilter. The FBI have advised home users to reboot their devices.

"The FBI on Friday issued a formal warning that a sophisticated Russia-linked hacking campaign is compromising hundreds of thousands of home

network devices worldwide and it is advising owners to reboot these devices in an attempt to disrupt the malicious software."

"The law enforcement agency said foreign cyber actors are targeting routers in small or home offices with a botnet — or a network of infected devices — known as VPNFilter."

28.05.18

Security Brief Asia

Trump cancelling North Korea summit will have 'cyber-retaliation'

It has been warned that if the US President Donald Trump cancels the meeting with North Korean leader Kim Jong Un then the US will suffer from a 'cyber-retaliation.'

"Headlines around the world have been painted with the news that Trump has cancelled a historic US-North Korea summit – which could have huge implications on the US's cybersecurity."

"It would have been the first time a sitting US president met a North Korean leader, but it seems not to be after North Korea released statements belittling US vice president Mike Pence."

30.05.18

Reuters

US warns again on hacks it blames on North Korea

The US Department of Homeland Security have issued their third warning and published technical details over a number of attacks which happened back in 2009 by the group "Hidden Cobra" which they have blamed on North Korea.

"The U.S. government on Tuesday released an alert with technical details about a series of cyber attacks it blamed on the North Korean government that stretch back to at least 2009."

"The warning is the latest from the Department of Homeland Security and the Federal Bureau of Investigation about hacks that the United States charges were launched by the North Korean government."

30.05.18

Web Africa

Kenya's war on cybercrime

Kenya have been suffering from a sustained rise in cyber attacks, in 2017 it cost the country Sh21.1 billion according to a 2017 Serianu study. The Government have responded and made the Computer Misuse and Cybercrimes Act law, which means cyber-criminals will now be reprimanded for their actions.

"Cyberattacks in Kenya are on the rise. There's barely a day that goes by where you don't hear about a major data breach or an organisation that has unsuspectingly fallen victim to ransomware, spear-phishing or impersonation fraud. The government has seen the urgency and on 16 May signed the Computer Misuse and Cybercrimes Act into law."

"And while most of the news coverage has focused on the perceived negatives of the legislation – including restrictions around freedom of expression and access to information - individuals should be pleased that cyber criminals will now face consequences."

30.05.18

Tech Central

Kenya cybercrime law opens door to privacy violations, censorship

Kenya's new Computer Misuse and Cybercrimes Act which became law on the 16th May 2018 have raised concerns that it restricts freedom of expression and access to information. This is because the new act criminalises hate speech and false publications however there is no definition to distinguish what constitutes as hate speech from speech that is protected under Kenya's existing laws.

"More and more Kenyans are connecting to the Internet, most frequently from mobile devices."

"There are, of course, big benefits to increased connectivity. These include the rise of mobile money transactions and access to loans. But there are downsides, too. The country has been targeted by hackers in several major attacks."

Privacy

No new items of relevance

Internet Inclusion

26.05.18

IT News Africa

Online mentoring consultancy helping African students get a dream college offer

An online tutor company called Crimson Education have announced they will expand their operations to South Africa to help address the skills gap in the country. Their consultancy has a network of over 2,000 mentors from all over the world.

"Crimson Education an online mentoring consultancy that helps build high school students' candidacy to apply for overseas universities has opened offices in South Africa. Crimson was started by two high-scholars Jamie Beaton and South Africa-born Sharndre Kushor in 2013 is currently operating in 17 cities around the world including South Africa."

"Crimson's entire business model is reliant on remote mentoring services –This model allows for students to tap into strong and powerful networks from anywhere in the world."

29.05.18

The Hill

Russia asks Apple to ban messaging app Telegram

Russia have urged American technology company Apple to remove Telegram from their app store after the messaging app refused to provide the Russian Government with access to their user's data**.**

"Russia is asking Apple to remove Telegram from its app store after the messaging app refused requests to give the government backdoor access to its platform."

"Russia had tried to ban Telegram earlier this year but is reportedly having a difficult time completely blocking the app within its borders."

29.05.18

The Guardian

[‘Blockchain technology key to economic development in Africa’]

According to experts at the Blockchain Africa Conference, blockchain technology which stores blocks of information that are identical across its network are key to unlocking technological development in Africa.

“As Blockchain Technology (BT) continues to have wider application across platforms including industries with unassailable results, Nigeria and Africa in general have been advised to embrace it to open up the continent for development.”

“Experts at the maiden edition of Blockchain Africa Conference organised by Fintech Worldwide Limited in association with Eka Consult in Lagos, agreed that with the current global trend, the technology has come to provide golden opportunities for development in the African continent.”

29.05.18

IT News Africa

[Founder and CEO of Future Nation Schools, Sizwe Nxasana to deliver a keynote at Education Innovation Summit 2018]

Sizwe Nxasana the Chief Executive of Future Nation Schools, an education group which seeks to be the leading learning group in Africa will be giving a speech at the upcoming Education innovation Summit to discuss the technological challenges facing the education sector.

“Sizwe Nxasana, the Founder and CEO of Future Nation Schools and Chairman of the National Student Financial Aid Scheme (NSFAS) will deliver a keynote on “The Future of Education” at the upcoming 3rd edition of the Education Innovation Summit set to take place at the Hilton Hotel in Sandton on 31 May 2018.”

“The summit is designed to bring together innovation leaders and educators to accelerate innovative thinking in education.”

28.05.18

IT News Africa

Enhancing science and IT learning in rural South Africa

A mobile science and IT lab has been given to the Mochudi Secondary School in Rural North West, South Africa which will help the students and teachers to develop their skills in science teaching and learning.

"Mochudi Secondary School in Rural North West, South Africa has become the beneficiary of a mobile science and IT Lab which is designed to help teachers and pupils."

"Many of the rural schools in South Africa need resources that reflect the futuristic innovation that will positively change lives."

30.05.18

The Guardian

Akeredolu commissions digital resource centre in Owo

Olurotimi Akeredolu, the Governor of Ondo State in Nigeria, has announced a new digital resource center which will be used to help improve the education and learning delivery in schools.

"The Governor of Ondo State, Olurotimi Akeredolu, has commissioned a state-of-the-art digital resource centre at Owo High School, Owo, Ondo State."

"The Digital Resource Centre which was donated by the President and Managing Director, CBC Emea Group of Companies and an alumnus of Owo High School, Foluso Falaye, is expected to improve the quality of education and learning delivery in the school."

30.05.18

The Guardian

Accenture commits $200m to digital skills development

Accenture, a leading global professional services company have announced $200 million to help disadvantaged individuals get jobs in the digital age by equipping them with job skills.

"Global management consulting and professional services firm, Accenture has voted more than $200 million over the next three years to help equip disadvantaged people with job skills for the digital age."

“The support, according to the company that provides strategy, consulting, digital, technology and operations services, is part of its vision to improve the way the world works and lives.”

Global Institutions

23.05.18

Council of Europe

Council of Europe co-operation with IT sector: two new partners

The European Internet Service Providers Association and the IT security and performance firm Cloudflare Another, have become the two latest members to join the Council of Europe's cooperation agreement to promote an open and safe internet. They join eight other technology firms including Apple, Facebook, Google, Microsoft, Kaspersky Lab and Orange and Telefónica.

"The Council of Europe´s Secretary General, Thorbjørn Jagland, today signed collaboration agreements - in the form of an exchange of letters – with the European Internet Service Providers Association (EuroISPA) and the IT security and performance firm Cloudflare to promote respect for human rights, democracy and the rule of law online."

"These new partners join another eight technology firms and six associations which entered into the same kind of co-operation agreement with the Council of Europe in November 2017."

Diary Dates

EuroDIG – 05.06.18-06.06.18

Tbilisi, Georgia

Data Centres Risk Radar – 24.06.18

London, England

TechUK Briefing on Cyber, PNT and the Maritime Sector – 04.06.18

London, England

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