



27 June 2018

Synopsis

Scroll to read full summaries with links to news articles.

Nepal are consulting with the **Telecom Regulatory Authority of India** to assess whether they should introduce a regulatory framework to make the delivery of the internet and **data services** fairer. They are considering a '**net neutrality**' policy which will regulate the way internet service providers deliver services in terms of speed-based discrimination and the pricing of internet traffic.

The **United States Treasury Department** are drafting legislation to limit the amount of **Chinese investment** into US technology firms. If put in place this would block firms with 25% of Chinese Ownership from buying US companies.

A group of lawmakers in the **US** have urged internet giant **Google** to end its partnership with Chinese phone maker **Huawei** on grounds that it poses a national security concern. This is because they fear the technology could be used by the **Chinese Government** to spy on the US.

Nine **European Union** states have announced their plans to create a new '**EU Cyber Rapid Response Force**' team to deal with **cyber threats**. The team is headed by Lithuania and includes Croatia, Estonia, France, Finland, the Netherlands, Romania and Spain.

The **EU Commission** have introduced legislation to deal with the problem of **data localization**. They have agreed to allow non-personal data to move across the bloc and have removed national laws that require companies to store data within a country's borders. This means companies can choose where in the EU they wish to store their data.

Greg Clark the UK Business Secretary has announced that the **UK Government** will be dedicating £1.3 bn to attracting the top talent and closing the **digital skills** gap.

The **UK** fear **US** President **Donald Trump**'s plans to talk with his **Russian** counterpart **Vladimir Putin** could have an impact on Trump's commitment to **cyber defence**, one of **NATO's** shared goals. Trump will be in **Europe** for a

NATO summit on July. The US President will then either meet Putin before the summit or after his UK visit two days later.

The Chair of the **US Federal Trade Commission**, **Joseph Simons** has said that he will investigate how big technology companies, including **Facebook** and **Google**, use their market power to potentially hurt rivals.

North American, **Britain** and **Asian** financial watchdogs have asked to be formally exempted from **European Union's** tough new **data privacy laws** in a bid to avoid the 'hampering of cross border investigations'. However, the EU is unlikely to provide such exemptions as they could potentially be used to illegitimately avoid its privacy safeguards.

A Draft **Data Protection** Bill will be published in **Kenya** by the end of this month and will focus on how organisations and businesses handle the personal data of Kenyans. The Minister of Information, Communication and Technology, **Joseph Mucheru** said, "we cannot ignore the fact that we have become a digital economy and therefore we need to have all the protections that are needed."

According to a new report released by the **General Household Survey 2017**, only one tenth of **South African** households have **access to the internet** at home. In Western Cape 25.7% have access, Gauteng, 16.5% and the lowest households with internet access were in Limpopo, 2.2% and Eastern Cape 3.5%.

Technology company **Microsoft** have announced their plans to transform **Nigerian schools** by gathering education leaders to discuss how to make schools more efficient by digitally transforming education and school management.

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

27 June 2018

Table of Contents

Synopsis	1
Europe	4
Internet governance.....	4
Cybersecurity	4
Privacy.....	6
Internet Inclusion	7
United States of America	10
Internet governance.....	10
Cybersecurity	10
Privacy.....	12
Internet Inclusion	13
Pan-Asia	15
Internet governance.....	15
Cybersecurity	16
Privacy.....	16
Internet Inclusion	18
Rest of the World	20
Internet governance.....	20
Cybersecurity	20
Privacy.....	21
Internet Inclusion	21
Global Institutions	23
Diary Dates	24

Europe

Internet governance

No new items of relevance.

Cybersecurity

22.06.18

The Independent

[Trump appears to be planning for a historic Putin summit](#)

The UK fear US President Donald Trump's plans to talk with his Russian counterpart Vladimir Putin could have an impact on Trump's commitment to cyber defence, one of NATO's shared goals. Trump will be in Europe for a NATO summit on July. The US President will then either meet Putin before the summit or after his UK visit two days later.

"As ties to traditional allies fray, US President Donald Trump seems to be gearing up for a major summit with Vladimir Putin."

"On Thursday, the Kremlin said it was 'aware' of a forthcoming Moscow visit by the White House's national security adviser, John Bolton. According to the Interfax news agency, that visit could come as early as next week, with Mr. Trump following soon thereafter."

26.06.18

Channel News Asia

[Ukraine says Russia hackers laying groundwork for massive strike](#)

According to Ukraine's Cyber Police Chief, Serhiy Demedyuk, Russia are bombarding Ukraine with cyber attacks, they are infecting Ukrainian companies and the Police Chief warns they are preparing for a massive strike.

"Hackers from Russia are infecting Ukrainian companies with malware to create so-called 'back doors' for a large coordinated attack, Ukraine's cyber police chief told Reuters on Tuesday, almost a year after a strike on Ukraine spread around the world."

“Affected companies range across various industries, such as banks or energy infrastructure. The pattern of the malware being rolled out suggests the people behind it want to activate it on a particular day, Serhiy Demedyuk said.”

27.06.18

The Register

[EU summons a cyber force into existence](#)

Nine European Union states have announced their plans to create a new ‘EU Cyber Rapid Response Force’ team to deal with cyber threats. The team is headed by Lithuania and includes Croatia, Estonia, France, Finland, the Netherlands, Romania and Spain.

“Lithuania's proposal that the European Union create an international cyber-force has been endorsed, and the effort already has seven countries on board.”

“The baltic country announced yesterday that EU member states have agreed to create “EU Cyber Rapid Response Force” teams, with a declaration of intent signed in Luxembourg yesterday by the EU Foreign Affairs Council.”

27.06.18

Euractiv

[Tackling hybrid threats, in Europe and the UK](#)

Mark Sedwill, the UK’s National Security Advisor, has called for EU leaders to tackle security issues including cyber threats, disinformation and hacking into elections during the June European Council on the 28th and 29th June.

“The June European Council is an opportunity to make sure we have the right measures in place to tackle hostile state threats to security such as cyber attacks, disinformation and meddling in elections, writes Mark Sedwill.”

“As the United Kingdom’s National Security Adviser, I am briefed every day on the activities of those who try to undermine the security of Britain and its allies.”

Privacy

20.06.18

Euractiv

[Negotiators reach quick agreement on law banning data localisation](#)

The EU Commission have introduced legislation to deal with the problem of data localization. They have agreed to allow non-personal data to move across the bloc and have removed national laws that require companies to store data within a country's borders. This means companies can choose where in the EU they wish to store their data.

"The legislation cracks down on data localisation and will open up the market for companies to choose where in the EU they store data. The European Commission has promoted the new rules as a way to make data storage easier and cheaper and has estimated that they will add 4% to the bloc's GDP by 2020."

"Data localisation restrictions are signs of protectionism for which there is no place in a single market. After free movement of people, goods, services and capital, we have made the next step with this agreement for a free flow of non-personal data to drive technological innovations and new business models and create a European data space for all types of data," Commission Vice-President Andrus Ansip said in a statement."

26.06.18

Channel NewsAsia

[North American, UK, Asian regulators press EU on data privacy exemption](#)

North American, Britain and Asian financial watchdogs have asked to be formally exempted from European Union's tough new data privacy laws in a bid to avoid the 'hampering of cross border investigations'. However, the EU is unlikely to provide such exemptions as they could potentially be used to illegitimately avoid its privacy safeguards.

"Financial watchdogs from North America, Britain and Asia are urgently seeking a formal exemption from the European Union's tough new data privacy law to avoid hampering cross-border investigations, regulatory officials told Reuters."

"Failure by the EU to explicitly exempt markets regulators from the bloc's General Data Protection Regulation (GDPR) could jeopardize international probes and enforcement actions in cases involving market manipulation and fraud, the officials warned."

Internet Inclusion

20.06.18

Sunday Express

[Cyber security: new scheme aims to bring more women into the industry](#)

A new cyber training scheme has been devised by Protection Group International (PGI), a security service in London, supported by Hawker Chase, a specialist cyber recruitment consultant, to address the shortage of women in cybersecurity. They will encourage women to use PGI's state-of-the-art Cyber Academy and training programme expertise to make it easier for women to transition into a cybersecurity profession after education.

"The chronic shortage of women in the cyber security is starting to being addressed with a new training scheme devised by Protection Group International (PGI), supported by Hawker Chase, a specialist cyber recruitment consultant."

"The cyber gap, the difference between the demand for cyber security professionals and their supply, is projected to reach 1.8million by 2022, with women currently only make up 20% of the industry's workforce."

20.06.18

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."

21.06.18

Computer Weekly

[Government sponsors diversity cyber academy](#)

The UK Department for Culture, Media and Sport have awarded a £50,000 grant to Immersive Labs, a Software as a Service Platform, to create a digital cyber academy for neurodivergent individuals. The academy will be aimed at helping neurodivergent individuals to upskill, developing the knowledge and technical skills required for a cyber career.

The UK government has awarded a grant for the establishment of a cyber academy to promote neurodiversity in the industry.

The Department for Digital, Culture, Media and Sport (DCMS) has awarded a £50,000 grant to Immersive Labs to create a digital cyber academy for neurodivergent individuals.

22.06.18

The Standard

[The UK government has invested £20 million into an Institute of Coding to improve digital skills](#)

The UK Government has formally launched the Institute of Coding (IoC), a body of universities and tech industry leaders, with a remit to develop the next generation of digital talent at degree level and above. The project seeks to promote a more diverse tech workforce by making courses available at apprenticeship, degree and short course level.

“Coding is one of the hottest skills to add to your CV at the moment.”

“But, according to a report by Tech Nation, over 50 per cent of the UK’s digital tech businesses say they are facing a shortage of skilled workers. This is why the UK government has launched a new Institute of Coding, a consortium of 25 universities and 60 businesses, who want to develop the next generation of tech talent.”

24.06.18

Public Technology

Government dedicates £1.3bn to attracting top science and tech talent

Greg Clark the UK Business Secretary has announced that the UK Government will be dedicating £1.3 bn to attracting the top talent and closing the digital skills gap.

“The Scottish Government has launched a £2m fund for businesses to improve their digital capabilities.”

“The money can be used in areas such as cybersecurity, data analytics, and software engineering, as well as to develop staff digital skills.”

25.06.18

Public Technology

Scottish Government offers £2m of interest-free loans to help boost firms’ digital skills

The Scottish Government will grant businesses a £2 million fund to be spent on improving their digital capabilities. The money will be used to improve their cybersecurity, data analytics, software engineering and to help develop their staff’s digital skills.

“It will enable businesses to cover the upfront costs of investing in digital technology and skills, and then repay the expenditure gradually.”

“Loans provided through the fund – which is called the Digital Development Loan – will be interest free, and the repayment can be spread over three to five years.”

United States of America

Internet governance

21.06.18

Reuters

[New FTC chair wants to look at market power of big internet companies](#)

The Chair of the U.S. Federal Trade Commission, Joseph Simons has said that he will investigate how big technology companies, including Facebook and Google, use their market power to potentially hurt rivals.

“Joseph Simons, the new chairman of the U.S. Federal Trade Commission (FTC), said on Wednesday that the agency would keep a close eye on big tech companies that dominate the internet.”

“Simons said the power of the big tech platforms - none of which he cited by name - raised new questions about competition and privacy. “It makes it very appropriate for it to be the subject of hearings and for us to get input on that,” he said at a question session with reporters.”

Cybersecurity

22.06.18

The Independent

[Trump appears to be planning for a historic Putin summit](#)

The UK fear U.S. President Donald Trump’s plans to talk with his Russian counterpart Vladimir Putin could have an impact on Trump’s commitment to cyber defence, one of NATO’s shared goals. Trump will be in Europe for a NATO summit in July. The U.S. President will then either meet Putin before the summit or after his UK visit two days later.

“As ties to traditional allies fray, US President Donald Trump seems to be gearing up for a major summit with Vladimir Putin.”

“On Thursday, the Kremlin said it was ‘aware’ of a forthcoming Moscow visit by the White House’s national security adviser, John Bolton. According to the Interfax news agency, that visit could come as early as next week, with Mr. Trump following soon thereafter.”

24.06.18

The Hill

[New fears over Chinese espionage grip Washington](#)

The United States lawmakers fear that Chinese espionage is penetrating the US, after hackers from China breached a Navy contractor's computer and gained vital information about submarine technology.

"Fresh concerns over Chinese espionage are gripping Washington as lawmakers fear Beijing is gaining sensitive details on U.S. technologies."

"Lawmakers are scrutinizing the Pentagon over its efforts to keep military secrets safe from hackers, after Chinese actors allegedly breached a Navy contractor's computer and collected data on submarine technology."

25.06.18

The Hill

[House passes bill to addressing industrial cybersecurity](#)

The House of Representatives has approved legislation that attempts to secure critical infrastructure from cyber attacks.

"House lawmakers approved legislation Monday aimed at securing technology used to power critical infrastructure from cyberattacks."

"The bill offered by Rep. Don Bacon (R-Neb.) would codify work the Department of Homeland Security is currently doing to identify cyber threats to industrial control systems and mitigate them. Industrial control systems are used to run critical services in the United States, including the electric grid, water systems, and manufacturing plants."

26.06.18

The Hill

[Senate panel moves to restore State cyber office](#)

The Senate Foreign Relations Committee have passed the Cyber Diplomacy Act which would see the creation of the Office of Cyberspace and the Digital Economy at the State Department, a high-level position that would oversee cyber policy abroad.

"A key Senate panel advanced a bill on Tuesday that aims to boost U.S. cyber diplomacy by creating a high-level position within the State Department to oversee cyber policy abroad."

“By a unanimous voice vote, the Senate Foreign Relations Committee passed ‘The Cyber Diplomacy Act,’ which would establish the Office of Cyberspace and the Digital Economy at State. The bill aims to boost engagement with other foreign nations on common cyber threats as well spread U.S. cyberspace interests abroad.”

Privacy

20.06.18

The Hill

[Lawmakers urge Google to drop partnership with Chinese phone maker Huawei](#)

A group of lawmakers in the US have urged internet giant Google to end its partnership with Chinese phone maker Huawei on grounds that it poses a national security concern. This is because they fear the technology could be used by the Chinese Government to spy on the US.

“A bipartisan group of lawmakers sent a letter to Google on Wednesday expressing concerns over the company’s partnership with the Chinese phone maker Huawei.”

“The group of senators and congressmen said that the partnership poses national security concerns, in step with previous efforts to keep Chinese tech firms, including ZTE and Huawei, from doing business in the U.S.”

22.06.18

Channel NewsAsia

[US Supreme Court restricts police on cellphone location data](#)

The U.S. Supreme Court have limited the amount of cellphone data pinpointing that the police in the US can obtain and now the police will need a court approved warrant to access the data.

“The U.S. Supreme Court on Friday imposed limits on the ability of police to obtain cellphone data pinpointing the past location of criminal suspects in a major victory for digital privacy advocates and a setback for law enforcement authorities.”

“In the 5-4 ruling, the court said police generally need a court-approved warrant to get the data, setting a higher legal hurdle than previously existed under federal law.”

26.06.18

Channel NewsAsia

[North American, UK, Asian regulators press EU on data privacy exemption](#)

North American, Britain and Asian financial watchdogs have asked to be formally exempted from European Union's tough new data privacy laws in a bid to avoid the 'hampering of cross border investigations'. However, the EU is unlikely to provide such exemptions as they could potentially be used to illegitimately avoid its privacy safeguards.

"Financial watchdogs from North America, Britain and Asia are urgently seeking a formal exemption from the European Union's tough new data privacy law to avoid hampering cross-border investigations, regulatory officials told Reuters."

"Failure by the EU to explicitly exempt markets regulators from the bloc's General Data Protection Regulation (GDPR) could jeopardize international probes and enforcement actions in cases involving market manipulation and fraud, the officials warned."

[Internet Inclusion](#)

22.06.18

The Guardian

[Microsoft, Sidmach to transform Nigerian schools](#)

Technology company Microsoft have announced their plans to transform Nigerian schools by gathering education leaders to discuss how to make schools more efficient by digitally transforming education and school management.

"Microsoft will be gathering education leaders in an event to address digital transformation in education, and introduce tools that aid effective school management and drive growth in quality of education across secondary schools in Lagos."

"The event, which holds on June 29, is targeted at Proprietors, Principals, Head Teachers and other high-level school administrators, and it aims to help schools create efficiency and effectiveness in school management."

25.06.18

Channel NewsAsia

[US plans limits on Chinese investment in US technology firms](#)

The United States Treasury Department are drafting legislation to limit the amount of Chinese investment into US technology firms. If put in place this would block firms with 25% of Chinese Ownership from buying US companies.

“The U.S. Treasury Department is drafting curbs that would block firms with at least 25 percent Chinese ownership from buying U.S. companies with ‘industrially significant technology,’ a government official briefed on the matter said on Sunday.”

“The official, whose comments matched a report by the Wall Street Journal, emphasized that the Chinese ownership threshold may change before the restrictions are announced on Friday.”

Pan-Asia

Internet governance

25.06.18

Medianama

[Nepal may introduce net neutrality regulations, consulting with TRAI](#)

Nepal are consulting with the Telecom Regulatory Authority of India to assess whether they should introduce a regulatory framework to make the delivery of the internet and data services fairer. They are considering a 'net neutrality' policy which will regulate the way internet service providers deliver services in terms of speed-based discrimination and the pricing of internet traffic.

"Nepal will soon be defining net neutrality when issuing licenses to telecom providers, the Himalayan Times reports. This makes the Nepal Telecom Authority the second regulator in south Asia that is taking action to enforce net neutrality rules, which are aimed at preventing discrimination in how ISPs deliver and price Internet traffic."

"The first regulator was TRAI, which has prohibited data tariffs that are discriminatory. TRAI has also issued recommendations to prevent speed-based discrimination. These recommendations are pending at the telecom department. Nepal's NTA is consulting with TRAI to finalize the policy."

25.06.18

Channel NewsAsia

[Fake news is a 'solvable problem' but tackling it with legislation could be difficult: Janil Puthuchery](#)

According to the Senior Minister of State for Communications and Information, Janil Puthuchery said false news online is a 'solvable problem' however introducing legislation in Singapore to tackle the issue will be difficult because it will affect all social media players not just Facebook.

"The Select Committee looking at the issue of deliberate online falsehoods is still deliberating on the matter but any possible law in Singapore, and its accompanying compliance costs, will affect all social media players and not just Facebook, said Senior Minister of State for Communications and Information Janil Puthuchery on Monday (Jun 25)."

“Mr. Puthuchery, speaking during a panel session on fake news, said from an engineering perspective, fake news is a “solvable problem” but acknowledged the difficulty in tackling it with legislation.”

Cybersecurity

No new items of relevance

Privacy

20.06.18

The Hill

[Lawmakers urge Google to drop partnership with Chinese phone maker Huawei](#)

A group of lawmakers in the U.S. have urged internet giant Google to end its partnership with Chinese phone maker Huawei on grounds that it poses a national security concern. This is because they fear the technology could be used by the Chinese Government to spy on the U.S.

“A bipartisan group of lawmakers sent a letter to Google on Wednesday expressing concerns over the company’s partnership with the Chinese phone maker Huawei.”

“The group of senators and congressmen said that the partnership poses national security concerns, in step with previous efforts to keep Chinese tech firms, including ZTE and Huawei, from doing business in the U.S.”

21.06.18

Reuters

[Japan firms slow to get compliant with new EU data privacy rules - Reuters poll](#)

According to a new poll, 26% of Japanese businesses have met some of the requirements expected under Europe’s strict new data privacy regulations. 8% said they were still working on providing affirmative consent, while 15% are yet to do anything.

“Around a quarter of Japanese businesses have made progress on meeting some of the easier requirements under Europe's new data privacy regulations while about another 20 percent plan to do so, a Reuters poll found.”

“But the number of companies who say they are currently equipped to deal with more onerous rules, such as those relating to data breaches and dealing with requests to provide personal data to customers - drops drastically to just a few.”

24.06.18

The Hill

[New fears over Chinese espionage grip Washington](#)

The United States lawmakers fear that Chinese espionage is penetrating the U.S .after hackers from China breached a Navy contractor's computer and gained vital information about submarine technology.

“Fresh concerns over Chinese espionage are gripping Washington as lawmakers fear Beijing is gaining sensitive details on U.S. technologies.”

“Lawmakers are scrutinizing the Pentagon over its efforts to keep military secrets safe from hackers, after Chinese actors allegedly breached a Navy contractor's computer and collected data on submarine technology.”

26.06.18

Channel NewsAsia

[North American, UK, Asian regulators press EU on data privacy exemption](#)

North American, Britain and Asian financial watchdogs have asked to be formally exempted from European Union's tough new data privacy laws in a bid to avoid the 'hampering of cross border investigations'. However, the EU is unlikely to provide such exemptions as they could potentially be used to illegitimately avoid its privacy safeguards.

“Financial watchdogs from North America, Britain and Asia are urgently seeking a formal exemption from the European Union's tough new data privacy law to avoid hampering cross-border investigations, regulatory officials told Reuters.”

“Failure by the EU to explicitly exempt markets regulators from the bloc's General Data Protection Regulation (GDPR) could jeopardize international probes and enforcement actions in cases involving market manipulation and fraud, the officials warned.”

Internet Inclusion

19.06.18

Channel NewsAsia

[Beijing subway to get 'bio-ID' tracking systems: Report](#)

Beijing have announced their plans to introduce 'bio-recognition technology' including facial recognition cameras and palm scanners to make it easier and quicker for passengers to flow through the subway at peak times.

"The Chinese capital, Beijing, is looking at introducing 'bio-recognition technology', including palm scanners and facial recognition cameras, to speed up passenger flow through subway stations at peak times, state media reported on Tuesday (Jun 19)."

"China is increasingly using surveillance technology for everything from bolstering domestic security to speeding up orders at fast-food restaurants. However, that kind of monitoring is stoking concerns from human rights groups that it is building a nationwide surveillance system to quell dissent."

20.06.18

Channel NewsAsia

[Silicon Valley-style coding boot camp seeks to reset Japan Inc.](#)

It has been six months since Code Chrysalis, a 12-week advanced coding school in Tokyo was established. Since then a dozen of students have graduated serving as a potential solution to Japan's digital skills gap.

"Barely six months after inaugurating a tiny software-coding boot camp in a basement in Tokyo, Silicon Valley transplant Kani Munidasa stood before some of Japan's top business leaders in February with a warning: software was threatening their future."

"A Sri Lankan native with a Japanese mother and wife, Munidasa was speaking at the invitation of Nobuyuki Idei, a former chief executive of Sony Corp."

25.06.18

Channel NewsAsia

[US plans limits on Chinese investment in US technology firms](#)

The United States Treasury Department are drafting legislation to limit the amount of Chinese investment into US technology firms. If put in place this would block firms with 25% of Chinese Ownership from buying US companies.

“The U.S. Treasury Department is drafting curbs that would block firms with at least 25 percent Chinese ownership from buying U.S. companies with “industrially significant technology,” a government official briefed on the matter said on Sunday.”

“The official, whose comments matched a report by the Wall Street Journal, emphasized that the Chinese ownership threshold may change before the restrictions are announced on Friday.”

Rest of the World

Internet governance

25.06.18

iAfrikan

[Kenya to publish Draft Data Protection Bill](#)

A Draft Data Protection Bill will be published in Kenya by the end of this month and will focus on how organisations and businesses handle the personal data of Kenyans. The Minister of Information, Communication and Technology, Joseph Mucheru said, “we cannot ignore the fact that we have become a digital economy and therefore we need to have all the protections that are needed.”

“Joseph Mucheru, Kenya's Minister of Information, Communication and Technology, has said that the Draft Data Protection Bill will be published during June 2018 for consideration and comment. The Draft Data Protection Bill will focus on how various businesses and organizations should handle the personal data of Kenyans.”

“Furthermore, the draft Bill is expected to outline and specify how the personal data should be collected, stored and distributed (shared).”

Cybersecurity

26.06.18

Channel News Asia

[Ukraine says Russia hackers laying groundwork for massive strike](#)

According to Ukraine's Cyber Police Chief, Serhiy Demedyuk, Russia are bombarding Ukraine with cyber attacks, they are infecting Ukrainian companies and the Police Chief warns they are preparing for a massive strike.

“Hackers from Russia are infecting Ukrainian companies with malware to create so-called 'back doors' for a large coordinated attack, Ukraine's cyber police chief told Reuters on Tuesday, almost a year after a strike on Ukraine spread around the world.”

“Affected companies range across various industries, such as banks or energy infrastructure. The pattern of the malware being rolled out suggests the people behind it want to activate it on a particular day, Serhiy Demedyuk said.”

Privacy

No new items of relevance

Internet Inclusion

21.06.18

MyBroadband

[Very few South Africans have Internet at home](#)

According to a new report released by the General Household Survey 2017, only one tenth of South African households have access to the internet at home. In Western Cape 25.7% have access, Gauteng, 16.5% and the lowest households with internet access were in Limpopo, 2.2% and Eastern Cape 3.5%.

“Statistics South Africa (Stats SA) released its General Household Survey 2017, which shows that only one-tenth of South African households have access to the Internet at home.”

“The report shows that home Internet access was most prevalent among households in the Western Cape (25.7%) and Gauteng (16.5%), and lowest in Limpopo (2.2%) and Eastern Cape (3.5%).”

22.06.18

The Guardian

[Microsoft, Sidmach to transform Nigerian schools](#)

Technology company Microsoft have announced their plans to transform Nigerian schools by gathering education leaders to discuss how to make schools more efficient by digitally transforming education and school management.

“Microsoft will be gathering education leaders in an event to address digital transformation in education, and introduce tools that aid effective school

management and drive growth in quality of education across secondary schools in Lagos.”

“The event, which holds on June 29, is targeted at Proprietors, Principals, Head Teachers and other high-level school administrators, and it aims to help schools create efficiency and effectiveness in school management.”

26.06.18

IT News Africa

[I-Innovate opens minds to Artificial Intelligence at Cape Town School](#)

I-Innovate a STEM educational specialist have announced a new programme in South Africa called the AI Family Challenge which will reach more than 20,000 learners in disadvantaged areas to bring together students, teachers and family members

“STE(A)M educational specialist, I-Innovate is bringing another 21st Century learning programme to South Africa to open up opportunities in our under-served school communities for learners to develop the talents and skills that are sorely needed in the Digital Age.”

“This month, Grade 3 to 7 learners from Heideveld Primary School and their families can step into the astounding world of Artificial Intelligence (AI) when they join a free 3-day initiative, the AI Family Challenge.”

27.06.18

The Guardian

[Technology hubs spread across Nigeria, may create more jobs](#)

More technology hubs are spreading across Nigeria, there are approximately 50 hubs in the country up from seven about five years ago.

“Nigeria’s technology space is getting more interesting! This is because more technology hubs are being established in the country, giving hope for a knowledge economy and increased job creations.

“The Guardian findings showed that there are now about 50 technology hubs in Nigeria, up from seven about five years ago. Further checks revealed that South West houses about 15; South East has two; South South is home to eight, while Northern Nigeria can boast of 12 hubs.”

Global Institutions

22.06.18

The Independent

[Trump appears to be planning for a historic Putin summit](#)

The UK fear US President Donald Trump's plans to talk with his Russian counterpart Vladimir Putin could have an impact on Trump's commitment to cyber defence, one of NATO's shared goals. Trump will be in Europe for a NATO summit on July. The US President will then either meet Putin before the summit or after his UK visit two days later

"As ties to traditional allies fray, U.S. President Donald Trump seems to be gearing up for a major summit with Vladimir Putin."

"On Thursday, the Kremlin said it was 'aware' of a forthcoming Moscow visit by the White House's national security adviser, John Bolton. According to the Interfax news agency, that visit could come as early as next week, with Mr. Trump following soon thereafter."

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

[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