IEEE

interel
COUNT ON US

IEEE

GLOBAL INTERNET POLICY MONITOR

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

17 October 2018

Synopsis

Scroll to read full summaries with links to news articles.

According to an industry body, **data privacy** rules in **Asia** are hindering the growth and spread of **financial technology**. They have urged the regulators to avoid an ‘exhaustive and prescriptive’ list of rules and allow companies to operate ‘confidently across borders and enter new markets.’

The Five Eyes, an intelligence alliance comprising of Australia, Canada, New Zealand, the UK and the USA have been sharing information about **China’s foreign activities** has been seen as a sign of a ‘broadening international front against Chinese influence operations and investments.’

Two US Senators, **John Cornyn** and **Mark Warner** have urged **Narendra Modi**, the Indian Prime Minister to change its strict data localisation laws because they represent “key trade barriers” between the **United States** and **India**.

Despite opposition from member states and legal experts, **Pierre Moscovici**, the EU Economic and Financial Affairs Commissioner has called for an EU-wide **digital tax** by Christmas.

According to **NATO** Assistant Secretary General for emerging security challenges, **Antonio Missiroli**, NATO will be “fully operational in cyber space in the same way it is in the sea, on land or in air” by 2023.

The Government’s **Digital Competition Panel**, led by former Obama Advisor **Jason Furman**, has opened a call for evidence into whether competition in the **UK** digital market is being “stifled by powerful tech giants.” A panel of experts will examine “the pros and cons for consumers of the current market set-up, where a small number of companies dominate digital markets and whether their accumulation of people’s data is holding back new companies that could offer people innovative products and services”.

The **Trump administration** has endorsed the Federal Communications Commission’s repeal of **net neutrality** rules, while a number of US Democrat members of Congress, including Senator Chuck Schumer and Nancy Pelosi, support the twenty-two states that are challenging the **FCC’s** ruling.

The **United States** have passed an important cyber bill called the **Cybersecurity and Infrastructure Security Agency Act** which will create a **cybersecurity** agency that has the same authority as the **Department for Homeland Security**.

The **Massachussets Institute of Technology** have announced plans to create a $1 billion collage completely dedicated to **AI, machine learning and data science**. This is the largest amount of funding by a US academic institute into **artificial intelligence**.

On Friday 5th October **Africa** held the fourth edition of the **'Africa Code Week'** in Johannesburg which has encouraged more than 1.8 million African youth to code and has facilitated **ICT education** into the school curriculum.

According to Nigeria **CommunicationsWeek** investigations **Nigeria** exchanges 110 gigabytes per second of traffic locally. This represents an increase of'10,000 percent over the past five years.'

According to a 2018 **ICT Skills Survey**, **South Africa** is not doing enough to prepare those leaving education to engage and fill important roles within the Country's ICT sector. Adrian Schofiel, Programme Consultant at the **Institute of information Technology Professionals** said, "although the government periodically makes statements about placing more emphasis on maths, science, technology subjects, we don't see that translated into action across the majority of schools."

The **United States** have offered to provide **NATO** with their cyber capabilities if the threat from **Russia** warranted it.

NATO's Chief Secretary General **Jens Stoltenberg** has urged **Russia** to stop its 'reckless' behaviour and has vouched to strengthen the alliance. He said, "Russia must stop its reckless pattern of behaviour, including the use of force against its neighbours, attempted interference in election processes, and widespread disinformation campaigns."

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

17 October 2018

Table of Contents

Europe

Internet governance

09.10.18

Euractiv

EU digital tax: MEPs call for higher rates

Members of the European Parliament Economic and Monetary Affairs Committee have urged the European Commission to increase the EU's digital tax which currently sits at a 3% levy on revenues.

"The European Commission should consider increasing the proposed rates in the controversial digital tax plans, MEPs from the European Parliament's Economic and Monetary Affairs committee suggested on Tuesday (9 October)."

"As part of the measures currently on the table, the Commission proposes to hit digital firms with total annual revenues of €750 million or above and yearly EU taxable revenues of €50 million, with a 3% levy on revenues."

10.10.18

Computer Weekly

Ofcom says government should lead on internet regulation

The Office of Communications, a Government approved regulatory and competition authority has urged the Government to create internet regulation and legislation that an independent body could enforce.

"Representatives from the telecoms regulator tell House of Lords that the government should build a framework for internet regulation that other bodies can follow and enforce."

"Internet regulation would be more effective if the government developed legislation that an independent body could enforce, representatives of Ofcom have told a House of Lords committee."

12.10.18

Euractiv

Digital tax to come by Christmas, Moscovici says

Despite opposition from member states and legal experts, Pierre Moscovici, the EU Economic and Financial Affairs Commissioner has called for an EU-wide digital tax by Christmas.

"The EU's Economic and Financial Affairs Commissioner Pierre Moscovici has rallied the cause for an EU-wide digital tax to be rolled out in time for Christmas, amid a raft of opposition on the plans from member states, legal experts and industry associations."

"Speaking to BBC News, Moscovici said on Thursday (11 October): "It's doable to have an agreement by Christmas… Why by Christmas? Because after that, we will enter into another timing, which will be the political cycle – first, Brexit will approach; second, there will be the European elections."

Cybersecurity

07.10.18

The Times

UK war-games cyber attack on Moscow

The UK military has staged a war game featuring a large-scale cyber blackout attack on Moscow, in response to a possible Russian military attack on the West. The cyber war games show the growing importance of cyber capabilities for the military.

"Defence chiefs have war-gamed a massive cyber-strike to black out Moscow if Vladimir Putin launches a military attack on the West, after concluding that the only other way of hitting back would be to use nuclear weapons."

"Senior security sources have told The Sunday Times they are concerned that Britain has a capability gap that has left commanders with too few weapons to meet Kremlin aggression short of firing a Trident nuclear missile."

11.10.18

Computer Weekly

Nato to be fully operational in cyber space by 2023

According to NATO Assistant Secretary General for emerging security challenges, Antonio Missiroli, NATO will be "fully operational in cyber space in the same way it is in the sea, on land or in air" by 2023.

"Nato has to conduct operational activities in cyber space in the same way as it does in the sea, on land or in air, according to Antonio Missiroli, Nato assistant secretary general for emerging security challenges."

"Nato's full operational capability in terms of cyber security is expected by 2023," he said in panel discussion on the future of Nato's cyber policy at the 2018 European Cybersecurity Forum in Krakow."

11.10.18

Parliament.uk

Cyber Security in the United Kingdom

Ahead of Lord Waverley's debate on UK cyber security in the House of Lords next week, the House of Commons library has published a briefing note to assist Peers in preparing for the discussion. The paper provides a very top-level outline of current UK cyber security policy and the related structures and processes within government, as well as a summary of the most prominent threats. Russia is mentioned several times, within the context of the most recent accusations from the UK Government about hacking activity.

"In the UK, cyber is categorised as a high priority risk to national security. Cyber threats come both from nation states and from criminal individuals or groups."

"The Government states that the lines between different threat actors continue to blur as individuals and groups learn from, hire and work with one another. Cyber threats to the UK include cyber terrorism; fraud and serious organised crime; espionage; and disruption of critical national infrastructure (CNI)."

14.10.18

Ministry of Defence

Global Strategic Trends The Future Starts Today

The Ministry of Defence has launched a report entitled ‘The Global Strategic Trends the Future Starts Today’, which evaluates the emerging threats posed by countries, with a section devoted to Russia. The document stipulates that Russia is continuing to increase its spending on specific capabilities such as cyber, which poses a risk to the UK because “Russia may develop a different ethical and legal framework for using these technologies compared with the West.”

“Purpose. Global Strategic Trends (GST) provides a strategic context for those in the Ministry of Defence (MOD), and wider government, who are involved in developing long-term plans, policies and capabilities.”

“Without an impartial strategic context there is a risk that planners, policymakers and capability developers would assume a future that supports their assumptions and bias.”

15.10.18

Euractiv

Italy resists EU push to impose sanctions over cyberattacks

Italy has urged the European Union not to impose sanctions or a penalty regime for states that engage in cyber espionage, as they fear this could lead to escalating tensions with Russia.

“Italy is resisting a European Union push to impose sanctions on states who carry out cyberattacks, a move that appears in line with Rome’s calls to de-escalate tensions with Russia but that could alienate Italy from its EU allies.”

“Diplomats said the sanctions plan is meant to strengthen EU defences and deterrence against cyberattacks, in particular from Russia, which has been in recent months at the centre of allegations of elections meddling in various Western states as well as security breaches conducted through electronic means.”

15.10.18

Computer Weekly

IoT firms sign up to UK security code of practice

The UK Department of Digital, Culture, Media and Sport and the UK National Cyber Security Centre have created a new ‘Voluntary Code of Practice’ for internet connected devices to help guide manufacturers to increase the security of their devices.

“Internet of things technology firms have begun signing up to a UK code of practice to strengthen the security of internet-connected devices. The code is expected to form the basis of an international standard.”

“The UK has published a voluntary code of practice (CoP) to help manufacturers boost the security of internet-connected devices that make up the internet of things (IoT).”

Privacy

12.10.18

Channel NewsAsia

Five Eyes intelligence alliance builds coalition to counter China

The Five Eyes, an intelligence alliance comprising of Australia, Canada, New Zealand, the UK and the USA have been sharing information about China’s foreign activities in a sign of a ‘broadening international front against Chinese influence operations and investments.’

“The five nations in the world's leading intelligence-sharing network have been exchanging classified information on China's foreign activities with other like-minded countries since the start of the year, seven officials in four capitals said.”

“The increased cooperation by the Five Eyes alliance - grouping Australia, Britain, Canada, New Zealand and the United States - with countries such as Germany and Japan is a sign of a broadening international front against Chinese influence operations and investments.”

15.10.18

Computer Weekly

Tech companies should not be under legal duty to remove terrorist material, says watchdog

According to Max Hill, the Independent reviewer of terrorism legislation, internet technology companies should not legally force companies to remove content online because it may 'interfere with the rights of innocent people' as it is not always easy to distinguish what material needs to be removed.

"The internet should not be a safe place for terrorists but making it compulsory for technology companies to trawl for radical content risks interfering with the rights of innocent people, says Max Hill QC, the independent reviewer of terrorism legislation."

"The UK should not follow the lead of other countries by introducing laws to force technology companies to remove extreme terrorist material from social media sites, says the UK's independent reviewer of terrorism legislation."

Internet Inclusion

08.10.18

Gov.uk

Cyber Skills Immediate Impact Fund

The Government has announced the launch of the Cyber Skills Immediate Impact Fund, which aims to increase the diversity and numbers of those working in the UK's cyber security sector. The fund makes grants available to a range of organisations to help more adults get into the cyber security profession and encourage talent from a range of backgrounds into cyber security roles. The fund is open to training providers and charities.

"The expanded Cyber Skills Immediate Impact Fund is now open for bids. The Fund aims to increase the diversity and numbers of those working in the UK's booming cyber security sector."

"The Cyber Skills Immediate Impact Fund (CSIIF) is being expanded to help a range of organisations quickly develop effective and sustainable initiatives that identify, train and place untapped talent from a range of backgrounds into cyber security roles."

11.10.18

The Independent

Multimillion pound government scheme for technical education is failing, report warns

A Government scheme called University Technical Collages, which specialise in cyber security and IT, has been launched across the UK over the past eight years. Companies including Microsoft, Fujitsu, Intel and Network Rail have partnered with UTC's offering live projects, and apprenticeship degrees. However, according to the Education Policy Institute think-tank, more than half of students who attend UTCs drop out between the ages of 16 and 17.

"A government scheme for technical education costing hundreds of millions of pounds is failing to deliver good results for students, according to a damning new report."

"More than half of students who attend University Technical Colleges (UTCs) - which take in pupils from the age of 14 to 19 - are dropping out between the ages of 16 and 17, the Education Policy Institute (EPI) found."

12.10.18

Computer Weekly

University vs Apprenticeship: The education debate

According to Alan Furley, Director of Specialist Tech and Engineering Recruitment Consultancy ISL, traditionally a degree is the preferred route into the technology industry, but many now believe apprenticeships are a more valuable path into the sector. He said, universities tend to teach "hard skills that aren't always contemporary or adaptable into a career, while at the same time the cost of a degree plus lost earning opportunities is ever growing."

"Traditionally, a degree is the preferred route into the technology industry, but many now believe an apprenticeship may be a more valuable path into the sector."

"Dissent appears to have been growing lately over whether getting a university education really is the best way to find a dream job in tech – or anywhere else, for that matter. For example, a study by the Chartered Institute of Personnel and Development revealed at the end of last year that a mere 52% of former students had found a graduate-level post within six months of leaving university."

16.10.18

Computer Weekly

More than half of women think their gender helps them pursue tech careers

According to Booking.com, nearly 60% of women believe their gender better places them to get jobs in the technology sector however more than 60% think there are no opportunities for progression because the sector is male dominated.

“A majority of women think being female helps them enter the tech sector, but career progression can be a different story, study shows.”

“Almost 60% of women believe their gender has a positive impact on their ability to pursue a technology career, according to research by Booking.com.”

16.10.18

Gov.uk

Digital Competition Expert Panel: Call For Evidence

The Government’s Digital Competition Panel, led by former Obama Advisor Jason Furman, has opened a call for evidence into whether competition in the UK digital market is being “stifled by powerful tech giants.” A panel of experts will examine “the pros and cons for consumers of the current market set-up, where a small number of companies dominate digital markets and whether their accumulation of people’s data is holding back new companies that could offer people innovative products and services”.

“To better understand the state of competition in the digital economy, the independent Digital Competition Expert Panel has launched a call for evidence.”

“At the request of the Chancellor, the expert panel is considering the potential opportunities and challenges the emerging digital economy may pose for competition and pro-competition policy. The panel is seeking evidence through this consultation to inform the recommendations it will make to government on any changes that may be needed.”

United States of America

Internet governance

03.10.18

Public Technology

US senators introduce legislation to boost government’s use of AI

The United States legislators have proposed new legislation to make it easier introduce artificial intelligence across the federal Government.

“Although ‘C-3PO isn’t yet a reality’, cross-party quartet wants to make it easier for federal agencies to adopt new technologies.”

“A cross-party group of US senators have put forward legislation designed to enable and promote the use of artificial intelligence across the federal government.”

13.10.18

Channel NewsAsia

US defends FCC's repeal of net neutrality rules

The Trump administration has endorsed the Federal Communications Commission’s repeal of net neutrality rules, while a number of US Democrat members of Congress, including Senator Chuck Schumer and Nancy Pelosi, support the twenty-two states that are challenging the FCC’s ruling.

“The Trump administration defended the Federal Communications Commission repeal of landmark open internet rules known as net neutrality, urging a federal appeals court to reject a challenge.”

“In a 167-page court filing late on Thursday, the Justice Department and FCC urged the court to reject the suit filed by 22 states, the District of Columbia, Mozilla Corp, Vimeo Inc, public interest groups and local governments.”

Cybersecurity

03.10.18

The Hill

US to offer NATO its cyber capabilities

The United States have offered to provide NATO with their cyber capabilities if the threat from Russia warranted it.

"The United States plans to announce in the coming days that it will offer its cyber capabilities to NATO amid concerns about Russia's use of its own cyber capabilities."

"We will formally announce that the United States is prepared to offer NATO its cyber capabilities if asked," said Katie Wheelbarger, the principal deputy assistant secretary of Defense for international security affairs, according to Reuters."

03.10.18

The Hill

Senate passes key cyber bill cementing cybersecurity agency at DHS

The United States have passed an important cyber bill called the Cybersecurity and Infrastructure Security Agency Act which will create a cybersecurity agency that has the same authority as the Department for Homeland Security.

"The Senate on Wednesday passed a key cyber bill that solidifies the Department of Homeland Security's role as the main federal agency overseeing civilian cybersecurity."

"Sen. Dan Sullivan (R-Alaska) asked for "unanimous consent" to pass the Cybersecurity and Infrastructure Security Agency Act, a bipartisan bill that will establish a cybersecurity agency that is the same stature as other units within DHS."

05.10.18

Channel NewsAsia

Pentagon sees China as 'growing risk' to US defence industry

According to a US Pentagon report, China poses a 'significant and growing risk' because China supplies certain materials and components that are vital to the US military.

“China represents a "significant and growing risk" to the supply of materials vital to the U.S. military, according to a new Pentagon-led report that seeks to mend weaknesses in core U.S. industries vital to national security.”

“The nearly 150-page report, seen by Reuters on Thursday ahead of its formal release on Friday, concluded there are nearly 300 vulnerabilities that could affect critical materials and components essential to the U.S. military.”

Privacy

12.10.18

Channel NewsAsia

Five Eyes intelligence alliance builds coalition to counter China

The Five Eyes, an intelligence alliance comprising of Australia, Canada, New Zealand, the UK and the USA have been sharing information about China’s foreign activities in a sign of a ‘broadening international front against Chinese influence operations and investments.’

“The five nations in the world's leading intelligence-sharing network have been exchanging classified information on China's foreign activities with other like-minded countries since the start of the year, seven officials in four capitals said.”

“The increased cooperation by the Five Eyes alliance - grouping Australia, Britain, Canada, New Zealand and the United States - with countries such as Germany and Japan is a sign of a broadening international front against Chinese influence operations and investments.”

13.10.18

Channel NewsAsia

US senators urge India to soften data localisation stance

Two US Senators, John Cornyn and Mark Warner have urged Narendra Modi, the Indian Prime Minister to change its strict data localisation laws because they represent “key trade barriers” between the United States and India.

“Two U.S. senators have called on Prime Minister Narendra Modi to soften India's stance on data localisation, warning that measures requiring it represent "key trade barriers" between the two nations.”

“In a letter to Modi dated Friday and seen by Reuters, U.S. Senators John Cornyn and Mark Warner - co-chairs of the Senate's India caucus that comprises

over 30 senators - urged India to instead adopt a "light touch" regulatory framework that would allow data to flow freely across borders."

16.10.18

Channel NewsAsia

Facebook to ban misinformation on voting in upcoming US elections

Internet giant Facebook have announced that they will ban all false reports and fact check them to ensure that the upcoming US elections are not influenced by false social media campaigns.

"California: Facebook will ban false information about voting requirements and fact-check fake reports of violence or long lines at polling stations ahead of next month's US midterm elections, company executives told Reuters, the latest effort to reduce voter manipulation on its service."

"The world's largest online social network, with 1.5 billion daily users, has stopped short of banning all false or misleading posts, something that Facebook has shied away from as it would likely increase its expenses and leave it open to charges of censorship."

Internet Inclusion

15.10.18

MIT Technology Review

MIT has just announced a $1 billion plan to create a new college for AI

The Massachusetts Institute of Technology have announced plans to create a $1 billion college completely dedicated to AI, machine learning and data science. This is the largest amount of funding by a US academic institute into artificial intelligence.

"One of the birthplaces of artificial intelligence, MIT, has announced a bold plan to reshape its academic program around the technology. With $1 billion in funding, MIT will create a new college that combines AI, machine learning, and data science with other academic disciplines. It is the largest financial investment in AI by any US academic institution to date."

"The new college of computing is being built with $350 million in funding from Stephen A. Schwarzman, the CEO and cofounder of Blackstone, a private equity firm."

Pan-Asia

Internet governance

No new items relevance

Cybersecurity

05.10.18

Channel NewsAsia

[Pentagon sees China as 'growing risk' to US defence industry]

According to a US Pentagon report, China poses a ‘significant and growing risk’ because China supplies certain materials and components that are vital to the US military.

“China represents a "significant and growing risk" to the supply of materials vital to the U.S. military, according to a new Pentagon-led report that seeks to mend weaknesses in core U.S. industries vital to national security.”

“The nearly 150-page report, seen by Reuters on Thursday ahead of its formal release on Friday, concluded there are nearly 300 vulnerabilities that could affect critical materials and components essential to the U.S. military.”

05.10.19

Channel NewsAsia

[Singapore can play ‘important role’ in cybersecurity for SEA region, says FireEye CEO]

According to the CEO FireEye, a cybersecurity company, Singapore can play an ‘important role’ in cybersecurity because it has “more centralised controls to prepare for and respond to cyber incidents than the US, and potentially any other nation out there”.

“Singapore can play an “important role” in cybersecurity for the Southeast Asian region, particularly in the area of thought leadership, said FireEye CEO Kevin Mandia on Thursday (Oct 4).”

“Mr Mandia told Channel NewsAsia in an interview on the sidelines of the company’s Cyber Defense Summit 2018 here that Singapore can lead the way for others in the region in terms of how to respond to cyber incidents and coming up with cyber rules for the region’s nations should it want to.”

Privacy

11.10.18

Channel NewsAsia

Data privacy rules spoiling fintech boom, says industry group

According to an industry body, data privacy rules in Asia are hindering the growth and spread of financial technology. They have urged the regulators to avoid an ‘exhaustive and prescriptive’ list of rules and allow companies to operate ‘confidently across borders and enter new markets.’

“Data privacy rules in Asia are limiting the spread of financial technology, an industry body said on Thursday, calling on regulators to set out broad principles rather than precise rules.”

“Companies around the world want to make better use of the large pools of data they have to both cut costs and offer additional services. But governments and regulators in Asia and elsewhere are tightening rules on how that data is used.”

12.10.18

Channel NewsAsia

Five Eyes intelligence alliance builds coalition to counter China

The Five Eyes, an intelligence alliance comprising of Australia, Canada, New Zealand, the UK and the USA have been sharing information about China’s foreign activities has been seen as a sign of a ‘broadening international front against Chinese influence operations and investments.’

“The five nations in the world's leading intelligence-sharing network have been exchanging classified information on China's foreign activities with other like-minded countries since the start of the year, seven officials in four capitals said.”

“The increased cooperation by the Five Eyes alliance - grouping Australia, Britain, Canada, New Zealand and the United States - with countries such as Germany and Japan is a sign of a broadening international front against Chinese influence operations and investments.”

13.10.18

Channel NewsAsia

US senators urge India to soften data localisation stance

Two US Senators, John Cornyn and Mark Warner have urged Narendra Modi, the Indian Prime Minister to change its strict data localisation laws because they represent "key trade barriers" between the United States and India.

"Two U.S. senators have called on Prime Minister Narendra Modi to soften India's stance on data localisation, warning that measures requiring it represent "key trade barriers" between the two nations."

"In a letter to Modi dated Friday and seen by Reuters, U.S. Senators John Cornyn and Mark Warner - co-chairs of the Senate's India caucus that comprises over 30 senators - urged India to instead adopt a "light touch" regulatory framework that would allow data to flow freely across borders."

Internet Inclusion

13.10.18

Channel NewsAsia

Alibaba's Jack Ma to open institute for tech entrepreneurs in Indonesia

Alibaba's Chinese e-commerce and retail giant have announced plans to open a new institute to train thousands of entrepreneurs in Indonesia, to help solve the skills gap.

"Jack Ma, executive chairman of China's Alibaba Group Holding, said on Saturday (Oct 13) he plans to open an institute to train thousands of tech entrepreneurs in Indonesia, where he is already an adviser to the government on e-commerce."

"Ma did not say when the Jack Ma Institute of Entrepreneurs would launch, but said the aim was to train 1,000 tech leaders a year over the next 10 years."

Rest of the World

Internet governance

No new items of relevance

Cybersecurity

07.10.18

The Times

UK war-games cyber attack on Moscow

The UK military has staged a war game featuring a large-scale cyber blackout attack on Moscow, in response to a possible Russian military attack on the West. The cyber war games show the growing importance of cyber capabilities for the military.

"Defence chiefs have war-gamed a massive cyber-strike to black out Moscow if Vladimir Putin launches a military attack on the West, after concluding that the only other way of hitting back would be to use nuclear weapons."

"Senior security sources have told The Sunday Times they are concerned that Britain has a capability gap that has left commanders with too few weapons to meet Kremlin aggression short of firing a Trident nuclear missile."

12.10.18

The Guardian

Nigeria, others face threats of cyber attacks

According to Check Point Software Technologies, which provide cybersecurity solutions across the globe, Nigeria is under threat from cybercriminals as they now see Africa as the place to launch cyber attacks on Government agencies, organisations and individuals.

"Check Point Software Technologies, a global provider of cybersecurity solutions, has revealed that African countries, Nigeria inclusive, are under heavy threat from cybercriminals."

"According to the report, the criminals now see African countries as a porous ground to launch cyber attacks on government agencies, organisations and individuals."

14.10.18

Ministry of Defence

Global Strategic Trends The Future Starts Today

The Ministry of Defence has launched a report entitled 'The Global Strategic Trends the Future Starts Today', which evaluates the emerging threats posed by countries, with a section devoted to Russia. The document stipulates that Russia is continuing to increase its spending on specific capabilities such as cyber, which poses a risk to the UK because "Russia may develop a different ethical and legal framework for using these technologies compared with the West."

"Purpose. Global Strategic Trends (GST) provides a strategic context for those in the Ministry of Defence (MOD), and wider government, who are involved in developing long-term plans, policies and capabilities."

"Without an impartial strategic context there is a risk that planners, policymakers and capability developers would assume a future that supports their assumptions and bias."

15.10.18

Euractiv

Italy resists EU push to impose sanctions over cyberattacks

Italy has urged the European Union not to impose sanctions or a penalty regime for states that engage in cyber espionage, as they fear this could lead to escalating tensions with Russia.

"Italy is resisting a European Union push to impose sanctions on states who carry out cyberattacks, a move that appears in line with Rome's calls to de-escalate tensions with Russia but that could alienate Italy from its EU allies."

"Diplomats said the sanctions plan is meant to strengthen EU defences and deterrence against cyberattacks, in particular from Russia, which has been in recent months at the centre of allegations of elections meddling in various Western states as well as security breaches conducted through electronic means."

Privacy

12.10.18

Channel NewsAsia

Five Eyes intelligence alliance builds coalition to counter China

The Five Eyes, an intelligence alliance comprising of Australia, Canada, New Zealand, the UK and the USA have been sharing information about China's foreign activities in a sign of a 'broadening international front against Chinese influence operations and investments.'

"The five nations in the world's leading intelligence-sharing network have been exchanging classified information on China's foreign activities with other like-minded countries since the start of the year, seven officials in four capitals said."

"The increased cooperation by the Five Eyes alliance - grouping Australia, Britain, Canada, New Zealand and the United States - with countries such as Germany and Japan is a sign of a broadening international front against Chinese influence operations and investments."

Internet Inclusion

07.10.18

IT News Africa

SAP Africa Code Week 2018 drives sustainable digital skills development

On Friday 5th October Africa held the fourth edition of the 'Africa Code Week' in Johannesburg which has encouraged more than 1.8 million African youth to code and has facilitated ICT education into the school curriculum.

"The fourth edition of the increasingly popular Africa Code Week, an initiative of SAP, kicked-off on Friday, 5 October at a function held in Johannesburg."

"Since its inception in 2015, Africa Code Week has introduced over 1.8 million African youth to coding skills in multiple African countries while facilitating the integration of ICT education in the school curriculum for more than 28,000 teachers and educators across the continent."

10.10.18

IT News Africa

South African-based Tari Labs unveils free online university

Tari Labs a startup in South Africa have unveiled a new free online university course called ‘Blockchain University’ to help address the growing skills gap in Africa.

“Tari Labs, a contributor to Tari, the South African-based blockchain protocol, has launched a free online university to help incubate open source projects and train blockchain developers, both locally and globally.”

“Tari Labs University aims to become a go-to destination for easily-accessible learning material for blockchain, digital currency and digital assets, from beginner to advanced level”, says Tari Lab’s senior contributor, Cayle Sharrock. By doing this, it hopes to ease a growing shortage of skilled blockchain and open source developers.”

12.10.18

The Guardian

Nigeria exchanges 110 gigabyte per second of traffic locally

According to Nigeria CommunicationsWeek investigations Nigeria exchanges 110 gigabytes per second of traffic locally. This represents an increase of ’10,000 percent over the past five years.’

“Nigeria internet ecosystem has achieved a significant milestone with the exchange of 110 gigabtye per second bandwidth of traffic locally, Nigeria CommunicationsWeek has learnt.”

“This feat represents an increase of 10,000 percent over the past five years and 40 percent of telecommunications operators and internet service providers (ISPs) traffic in the country.”

17.10.18

Web Africa

SA's education system can't fill ICT skills gap

According to a 2018 ICT Skills Survey South Africa is not doing enough to prepare those leaving education to engage and fill important roles within the Country’s ICT sector. Adrian Schofiel, Programme Consultant at the Institute of information Technology Professionals said, "although the government periodically makes statements about placing more emphasis on maths, science, technology subjects, we don't see that translated into action across the majority of schools.”

“South Africa is not doing nearly enough to ready school-leavers to engage and fill important vacant roles within the country's ICT sector.”

“Information security and cyber security skills remain at the top of the priority list and there are new priorities for emerging skill sets including AI, IOT and payment systems.”

Global Institutions

03.10.18

The Hill

US to offer NATO its cyber capabilities

The United States have offered to provide NATO with their cyber capabilities if the threat from Russia warranted it.

“The United States plans to announce in the coming days that it will offer its cyber capabilities to NATO amid concerns about Russia's use of its own cyber capabilities.”

“We will formally announce that the United States is prepared to offer NATO its cyber capabilities if asked,” said Katie Wheelbarger, the principal deputy assistant secretary of Defense for international security affairs, according to Reuters.”

04.10.18

Channel NewsAsia

Russia must stop cyber attacks on West: NATO's Stoltenberg

NATO’s Chief Secretary General Jens Stoltenberg has urged Russia to stop its ‘reckless’ behaviour and has vouched to strengthen the alliance. He said, "Russia must stop its reckless pattern of behaviour, including the use of force against its neighbours, attempted interference in election processes, and widespread disinformation campaigns."

“NATO's chief vowed on Thursday to strengthen the alliance's defences against attacks on computer networks that Britain said are directed by Russian military intelligence, also calling on Russia to stop its "reckless" behaviour.”

"Russia must stop its reckless pattern of behaviour, including the use of force against its neighbours, attempted interference in election processes, and widespread disinformation campaigns," NATO Secretary-General Jens Stoltenberg said in a statement after Britain and the Netherlands said they had evidence of Russian cyber attacks.”

11.10.18

Computer Weekly

Nato to be fully operational in cyber space by 2023

According to NATO Assistant Secretary General for emerging security challenges, Antonio Missiroli, NATO will be "fully operational in cyber space in the same way it is in the sea, on land or in air" by 2023.

"Nato has to conduct operational activities in cyber space in the same way as it does in the sea, on land or in air, according to Antonio Missiroli, Nato assistant secretary general for emerging security challenges."

"Nato's full operational capability in terms of cyber security is expected by 2023," he said in panel discussion on the future of Nato's cyber policy at the 2018 European Cybersecurity Forum in Krakow."

Diary Dates

Women in Tech Council – 20.09.18

London England

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

Sacramento, USA

ISC2 Secure Summit Toronto – 01.10.18

Toronto, Canada

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

Muscat, Oman