29 March 2017

Synopsis

Scroll to read full summaries with links to news articles.

There has been a concerted effort in the **EU** this week to introduce legislation to increase the ability of law enforcement to access data stored on secure messaging sites like **WhatsApp**. EU Justice Commissioner **Věra Jourová** has suggested new measures will be drafted in June, whilst the UK Home Secretary has convened a board of technology experts to propose solutions after the terrorist behind last week's Westminster attack was found to have used WhatsApp.

NATO have announced this week that they will invest €3billion in improving satellite bandwidth and **cybersecurity** across the alliance. Further details of the contracts will be announced at the April **Defence Conference** in Ottawa, **Canada**.

In the **UK** the Government's auditing body, the **NAO**, has published a report on the nature of the **digital skills** gap within the government. The findings argue that 2,000 expert digital staff will be required in the next five years in order to deal with the increasingly complex and ambitious nature of **digital projects**.

The **United States** has moved closer to naming the perpertrators of the **Bangladesh** Bank **cyber attack** that led to the theft $81 million. It has been suggested by commentators that the US is moving closer to publicly charging **North Korea** and **Chinese** accomplaces with responsibility for the heist.

The Attorney General of **New York** has disclosed that during 2016, **data breaches** in the state increased by over 60%, with the personal data of over 1.6million citizens being breached.

The House of Representatives has voted this week to repeal **privacy laws** that had prevented **Internet Service Providers** from selling the customer information, including browsing histories of clients.

Vietnam has reached out to **India** for guidance on **e-governance** as the Government looks at how it can emulate the Digital India implemented by Prime Minister **Narendra Modi**.

Ministers from the **Indonesian** Ministry of Communications and Information have announced that developing countries will back Indonesia's proposal for extended discussions on **cybersecurity** at the 2017 World Telecommunication Development Conference in Bali.

In **Singapore** the country's telecommunications companies are preparing to shut down existing **2G networks** in the first three weeks of April, in order to increase the provision of higher speed **3G** and **4G** networks across the country.

In **Nigeria** the National Communications Commission has launched a public consultation on the development of a **code of practice** for an **open internet**.

The **New Zealand** government has produced its first report into the implementation of its new **cybersecurity** strategy, in which it calls for greater cooperation with industry in order to fully realise its objectives.

Avanti Communications has announced that it will work with Governments and non-state actors in Sub-Saharan **Africa** to improve **internet access** in rural communities, through the use of its eco wi-fi technology.

The **ITEMS International** consultancy have produced a draft report into the **ICANN At-Large Advisory Committee**, in which they find the body is not fit for its intended purpose. The draft report is now available for public comment.

IEEE Global Internet Policy Monitor

29 March 2017

Table of Contents

Disclaimer: Please note that this monitor is a summary of news sources and does not reflect the official views of IEEE.

Europe

Internet governance

No new items of relevance

Cybersecurity

27.03.17

Politico

NATO plans €3 billion investment in satellite bandwidth, cybersecurity

NATO have announced that it will spend €3billion on the development of satellite communications and cybersecurity within the alliance. The money will be put towards the defence of NATO outposts and to improve the existing standards amongst member states.

"As security threats move online, the NATO Communications and Information Agency wants to strengthen network capabilities.

To that end, the alliance plans to invest around €3 billion in satellite bandwidth and stronger cybersecurity, a NATO official confirmed today.

The contracts for the expansion will be presented in Ottawa, Canada's capital, at an April defense conference.

Advanced software to help coordinate across NATO forces will cost around €180 million, while €800 million will go to the alliance's air and missile defense infrastructure."

28.03.17

Euractiv

Europe struggles to tackle cyber attacks in aviation

Experts within the European aviation sector have reported to Euractiv that not enough is being done too tackle cybersecurity issues in their sector. A major issue barring improvements in this area is the level of disagreement between EU member states on the necessary levels of cooperation.

"Cyber threats to the aviation sector are rapidly becoming a major issue for airlines, aircraft manufacturers and authorities. But Europe is finding legacy

problems and new challenges to address cyber risks for its air transportation systems.

Sources consulted by EURACTIV.com describe a fragmented landscape, with a poor understanding of the threat by officials, and substantial differences within the industry when it comes to the involvement of the EU.

"For the time being, it is extremely difficult to exchange information," said Pascal Andrei, who has been responsible for aircraft security at Airbus for fifteen years."

Privacy

27.03.17

SC Magazine

UK official: Backdoor needed into WhatsApp

The UK's Home Secretary Amber Rudd has called for greater access to secure messaging services for law enforcement. Ms Rudd made the statement following the terror attack on Parliament last week, in which the attacker communicated on the WhatsApp messaging service in the minutes before attacking.

"Following the terror attack on Parliament last week, home secretary Amber Rudd has suggested law enforcement must be able to listen in to WhatsApp conversations, as British-born Khalid Masood, who carried out the attack, is said to have used WhatsApp moments before murdering pedestrians with his car, and stabbing an unarmed police officer to death.

Speaking on BBC One's Andrew Marr show, Rudd spoke of an era when law enforcement would "steam open envelopes, or just listen in on phones, when they wanted to find out what people were doing", adding: "We need to make sure that our intelligence services have the ability to get into encrypted situations like WhatsApp."

27.03.17

The Independent

Ex-cyber security chief says Government is 'using' Westminster attack to grab unnecessary spying powers

Major General Jonathan Shaw, the UK's former cybersecurity chief for the Ministry of Defence has claimed that the Government are using last week's terror attack on Parliament to increase spying powers unnecessarily.

"The Ministry of Defence's former cyber security chief has accused the Government of trying to "use" the devastating Westminster attack to grab unnecessary and intrusive surveillance powers.

Major General Jonathan Shaw said ministers were attempting to "use the moment" to push for security services having more control, despite there being only a weak case for it.

Home Secretary Amber Rudd has turned up the heat on internet firms, saying it is "completely unacceptable" that authorities cannot look at encrypted social media messages of attacker Khalid Masood, but her words come as debate continues over allowing spy agencies further intrusive powers – only last year Parliament granted them sweeping new capabilities."

28.03.17

SC Magazine

Microsoft president takes stand against turning over data

Microsoft President Brad Smith has stated in an interview that Microsoft will continue to retain customer data unless legally compelled by law enforcement to hand over data.

"Microsoft will continue its hard-line stance against handing over customer data to any government unless it is "legally compelled to," company President Brad Smith reiterated in an interview with a U.K. news outlet.

"We will not help any government, including our own, hack or attack any customer anywhere," Smith said in an interview Monday with the U.K.'s ITV News, advocating for strict limits to the data governments can obtain from private citizens.

In age when law enforcement is pushing for ever-increasing access to the private communications of citizens and corporations, in particular technology companies, Microsoft has said it wouldn't cave to demands from intelligence agencies to automatically provide access to the data of its users."

29.03.17

EurActiv

EU to propose new rules targeting encrypted apps in June

The EU's Justice Commissioner Věra Jourová has announced that new EU wide legislation and other regulatory measures will be introduced in June of this year to provide greater police access to encrypted messagins services like WhatsApp.

"The European Commission will propose new measures in June to make it easier for police to access data on encrypted internet apps like WhatsApp, EU Justice Commissioner Věra Jourová said yesterday (28 March), heeding calls from national interior ministers.

Jourová said she will announce "three or four options" including binding legislation and voluntary agreements with companies to allow law enforcement authorities to demand information from internet messaging apps "with a swift, reliable response".

Non-legislative measures will be provisional "to have a quick solution", since negotiations over EU laws can drag on for years before they are passed."

Internet Inclusion

27.03.17

Silicon UK

NAO Study Finds 'Urgent' Government Digital Skills Gap

The UK's National Audit Office has published a report on the nature of the digital skills gap within the government. The findings argue that 2,000 expert digital staff will be require in the next five years in order to deal with the increasingly complex and ambitious nature of digital projects.

"At least 2,000 digital staff are needed within the next five years, and probably far more – and the private sector won't be any help, the NAO warns

The government's planning to provide itself with specialised skills isn't keeping pace with the scale of the challenges that lie ahead, including the delivery of ever-more ambitious digital projects, requiring a more "urgent" response, according to the National Audit Office (NAO).

The NAO's "Capability in the Civil Service" report found that in addition to scarce project planning, benefits realisation and contract management skills, government departments say they will need an additional 2,000 digital staff within five years, at an annual cost of between £145 and £245 million. Skills gap"

United States of America

Internet governance

24.03.17

SC Magazine

U.S. expected to charge North Korea for role in Bangladesh Bank digital heist

The United States has moved closer to naming the perpertrators of the Bangladesh Bank cyber attack that led to the theft $81 million. It has been suggested by commentators that the US is moving closer to publicly charging North Korea and Chinese accomplaces with responsibility for the heist.

“The Federal Bureau of Investigation believes that North Korea is responsible for the breach.

U.S. prosecutors are reportedly building a case against North Korea to examine the nation's possible role in the 2016 Bangladesh Bank digital heist which resulted in the theft of $81 million.

In the February 2016 incident, hackers breached Bangladesh Bank's system and used the SWIFT messaging network to request nearly $1 billion from its account at the New York Fed. While the majority of requests where declined after a typo triggered suspicion, $81 million dollars' worth of the malicious requests were approved.”

Cybersecurity

27.03.17

SC Magazine

New York data breaches rise by 60% due to hacking and insiders

The Attorney General of New York has disclosed that during 2016, data breaches in the state increased by over 60%, with the personal data of over 1.6million citizens being breached.

“New York firms have been required to report breaches under state law since 2005

New York data breaches have reached new heights according to the state's Attorney General Eric Schneiderman. Security breaches skyrocketed by 60 percent in 2016.

Firms reported 1,300 breach incidents involving the data of 1.6 million New York state residents. Hacking was the prime cause, appearing in 40 percent of reports. Insider breaches followed, constituting 37 percent of breaches. The remainder compriseda variety of causes including device theft and 'merchant missteps'."

27.03.17

Politico

NATO plans €3 billion investment in satellite bandwidth, cybersecurity

NATO have announced that it will spend €3billion on the development of satellite communications and cybersecurity within the alliance. The money will be put towards the defence of NATO outposts and to improve the existing standards amongst member states.

"As security threats move online, the NATO Communications and Information Agency wants to strengthen network capabilities.

To that end, the alliance plans to invest around €3 billion in satellite bandwidth and stronger cybersecurity, a NATO official confirmed today.

The contracts for the expansion will be presented in Ottawa, Canada's capital, at an April defense conference.

Advanced software to help coordinate across NATO forces will cost around €180 million, while €800 million will go to the alliance's air and missile defense infrastructure."

28.03.17

The Hill

DHS misses deadline to submit cyber strategy to Congress

The deadline for the Department of Homeland Security's cyber strategy has been missed by the department, who have passed the draft strategy to the Trump Administration for its input. The department has already acknowledged that it could take the Whitehouse several months to approve the document.

"The Department of Homeland Security (DHS) has missed a deadline for submitting a new cybersecurity strategy to Congress, a department official acknowledged on Tuesday.

The DHS was required by annual defense policy legislation passed in December to spell out a departmentwide cybersecurity strategy by last week. Rep. Cedric

Richmond (D-La.) signaled at a hearing on Tuesday morning that members of a congressional panel with oversight of the DHS had yet to receive the strategy."

Privacy

24.03.17

SC Magazine

FBI Director Comey advocates for weakening of security

The Director of the FBI James Comey, has suggested that there should be an international lowering of security standards for encrypted communications to increase the ease with which law enforcement can conduct surveillance on suspects.

"FBI director James Comey advocated for an easing of security mechanisms so that law enforcement worldwide would have an easier time snooping on encrypted communications, according to a report from IDG News Service.

Speaking at a conference on Thursday at the University of Texas at Austin, Comey intimated that the U.S. might collaborate with other nations on a framework for creating legal access to encrypted tech devices."

28.03.17

SC Magazine

Microsoft president takes stand against turning over data

Microsoft President Brad Smith has stated in an interview that Microsoft will continue to retain customer data unless legally compelled by law enforcement to hand over data.

"Microsoft will continue its hard-line stance against handing over customer data to any government unless it is "legally compelled to," company President Brad Smith reiterated in an interview with a U.K. news outlet.

"We will not help any government, including our own, hack or attack any customer anywhere," Smith said in an interview Monday with the U.K.'s ITV News, advocating for strict limits to the data governments can obtain from private citizens.

In age when law enforcement is pushing for ever-increasing access to the private communications of citizens and corporations, in particular technology companies, Microsoft has said it wouldn't cave to demands from intelligence agencies to automatically provide access to the data of its users."

29.03.17

SC Magazine

House votes to repeal FCC privacy laws for ISPs

The House of Representatives has voted this week to repeal privacy laws that had prevented Internet Service Providers from selling the customer information, including browsing histories of clients.

"Internet service providers (ISPs) soon will be able to sell their customers' data -- including their browsing histories -- without their consent after the House voted Tuesday to rout the Federal Communications Commission's broadband privacy rules.

The House vote, which saw 15 Republicans break from party lines to oppose the measure, followed a thumbs up from the Senate earlier in the month.

"Today Congress proved once again that they care more about the wishes of the corporations that fund their campaigns than they do about the safety and security of their constituents," according to Fight for the Future Campaign Director Evan Greer. "Gutting these privacy rules won't just allow Internet Service Providers to spy on us and sell our personal information, it will also enable more unconstitutional mass government surveillance, and fundamentally undermine our cybersecurity by making our sensitive personal information vulnerable to hackers, identity thieves, and foreign governments."

Internet Inclusion

27.03.17

Nextgov

IT Modernisation bill could be reintroduce in Congress this week

Republican Congressman Will Hurd appears set to reintroduce to Congress a bill focused on the modernisation of IT systems in the Federal government. The bill had passed the House in the last session but failed to pass the Senate during the lame duck period.

"One of the tech-savviest congressmen is ready to reintroduce legislation to tackle one of the federal government's greatest technology problems.

Sources on Capitol Hill tell Nextgov Rep. Will Hurd, R-Texas, could this week introduce a tweaked version of the Modernizing Government Technology Act, which passed the House in September but stalled in the Senate during the lame-duck session."

Pan-Asia

Internet governance

24.03.17

SC Magazine

U.S. expected to charge North Korea for role in Bangladesh Bank digital heist

The United States has moved closer to naming the perpertrators of the Bangladesh Bank cyber attack that led to the theft $81 million. It has been suggested by commentators that the US is moving closer to publicly charging North Korea and Chinese accomplaces with responsibility for the heist.

“The Federal Bureau of Investigation believes that North Korea is responsible for the breach.

U.S. prosecutors are reportedly building a case against North Korea to examine the nation's possible role in the 2016 Bangladesh Bank digital heist which resulted in the theft of $81 million.

In the February 2016 incident, hackers breached Bangladesh Bank's system and used the SWIFT messaging network to request nearly $1 billion from its account at the New York Fed. While the majority of requests where declined after a typo triggered suspicion, $81 million dollars' worth of the malicious requests were approved.”

28.03.17

Channel News Asia

VPN users in China megacity Chongqing face fines

The Chinese city of Chongqing has announced that it will look to fine any citizens caught using VPN’s to avoid the country’s “Great Firewall”.

“People in the Chinese megacity Chongqing could be fined for using VPNs to jump over the country's "Great Firewall" that blocks access to forbidden websites from Google to Facebook.

The punishment would be meted out to people using virtual private networks to access banned sites for commercial purposes, but Amnesty International said the wording was vague enough that it could affect any business or individual.”

Hindustan Times

28.03.17

Vietnam may emulate Digital India, seeks cooperation on e-governance

Vietnam has reached out to India for guidance on e-governance as the Government looks at how it can emulate the Digital India implemented by Prime Minister Narendra Modi.

"Vietnam on Tuesday sought cooperation from India in various fields, including cyber security and e-governance, to steer the country towards economic development on the lines of Prime Minister Narendra Modi's Digital India and e-governance initiatives.

The south-east Asian country joined a number of others, including the US, Japan, South Korea, the UK, Canada, Australia, Malaysia, Singapore and Uzbekistan, that have favoured India's Digital India and e-governance initiatives.

A Vietnamese delegation led by the country's information and communication minister Truong Minh Tuan met Union IT minister Ravi Shankar Prasad."

Cybersecurity

24.03.17

The Jakarta Post

Developing countries support cybersecurity: Official

Ministers from the Indonesian Ministry of Communications and Information have announced that developing countries will back Indonesia's proposal for extended discussions on cybersecurity at the 2017 World Telecommunication Development Conference in Bali.

"The Communications and Information Ministry's International Cooperation Center head, Ikhsan Baidirus, said developing countries had agreed to give close attention to the strengthening of cybersecurity during the regional preparatory meeting for 2017 World Telecommunication Development Conference in Bali.

"Indonesia's proposal on follow-up discussions about cybersecurity issues has received wide support from developing countries. Cybersecurity is not on the International Telecommunication Union [ITU] agenda but we are striving to put it in its programs," he said as quoted by Antara after the closing of the meeting in Legian on Thursday.

The meeting aims to unite the common interests of countries in the Asia-Pacific. All aspirations will be brought to the World Telecommunication Development

conference in Buenos Aires, Argentina, in October. Representatives of 29 ITU member countries from the Asia-Pacific attended the Bali meeting."

MIS Asia

29.03.17

China faces cybersecurity threats beyond their capabilities

Mastercard has produced a White Paper in which it identifies several cybersecurity threats currently outside the capabilities of Chinese businesses and citizens. The paper specifically references the impact that IoT cybersecurity threats will play in the future, particularly to small and medium sized enterprises.

"China's individuals and small firms are embracing the digital economy, but they are facing cybersecurity threats beyond their capabilities, according to a whitepaper by Mastercard.

The whitepaper indicates that digital technologies can help China unlock meaningful improvements in economic growth and development."

MIS Asia

30.03.17

CyberSecurity Malaysia in Asia Pacific drill to combat DDOS attacks

A major cybersecurity drill designed to improve reactions to DDOS attacks has taken place in the Asia Pacific region with Computer Emergency Response and Computer Security Incident Response teams from 22 countries participating.

"National digital security specialist CyberSecurity Malaysia has taken part in an Asia Pacific drill to test preparedness for DDOS attacks.

Themed 'Emergence of a New Distributed Denial of Service (DDoS) Threat,' this year's Asia Pacific Computer Emergency Response Team's (APCERT) drill tested different response capabilities of leading Computer Security Incident Response Teams (CSIRT) from the Asia Pacific economies."

Privacy

28.03.17

SC Magazine

Microsoft president takes stand against turning over data

Microsoft President Brad Smith has stated in an interview that Microsoft will continue to retain customer data unless legally compelled by law enforcement to hand over data.

“Microsoft will continue its hard-line stance against handing over customer data to any government unless it is "legally compelled to," company President Brad Smith reiterated in an interview with a U.K. news outlet.

"We will not help any government, including our own, hack or attack any customer anywhere," Smith said in an interview Monday with the U.K.'s ITV News, advocating for strict limits to the data governments can obtain from private citizens.

In age when law enforcement is pushing for ever-increasing access to the private communications of citizens and corporations, in particular technology companies, Microsoft has said it wouldn't cave to demands from intelligence agencies to automatically provide access to the data of its users.”

Internet Inclusion

29.03.17

Out-Law

Singapore telcos to begin '2G' shutdown on 1 April

In Singapore the country’s telecommunications companies are preparing to shut down existing 2G networks in the first three weeks of April, in order to increase the provision of higher speed 3G and 4G networks across the country

“M1, Singtel and StarHub will complete the shutdown of 2G networks in stages. The work is scheduled to be completed by 18 April

The move will allow spectrum currently used to support 2G services to be used instead for the provision of higher speed '3G', '4G' or more advanced mobile services, according to a statement issued by the MNOs and the Infocomm Media Development Authority of Singapore.”

29.03.17

Straits Times

10,000 public servants to receive data science training under GovTech-NUS tie-up

The Government of Singapore and the National University have signed a five year Memorandum of Intent to provide data science training to 10,000 public servents as part of plans to develop digital skills within the Government.

"About 10,000 public servants will receive data science training to quicken Smart Nation efforts.

This will take place under a five-year Memorandum of Intent (MOI) signed by Government Technology Agency of Singapore (GovTech) and the National University of Singapore (NUS) on Wednesday (March 29)."

Rest of the World

Internet governance

24.03.17

The Guardian (Nigeria)

NCC seeks inputs on internet code of practice

In Nigeria the National Communications Commission has launched a public consultation on the development of a code of practice for an open internet.

"Nigerian Communications Commission (NCC) has asked stakeholders in the Nigerian telecom industry, as well as the general public to contribute in the development of a code of practice in support of an open internet.

NCC said the establishment of internet industry code of practice is part of its Internet Governance function, but says it favours a multi-stakeholder model of engagement in the process of policy development for the Internet Governance."

Cybersecurity

24.03.17

The Jakarta Post

Developing countries support cybersecurity: Official

Ministers from the Indonesian Ministry of Communications and Information have announced that developing countries will back Indonesia's proposal for extended discussions on cybersecurity at the 2017 World Telecommunication Development Conference in Bali.

"The Communications and Information Ministry's International Cooperation Center head, Ikhsan Baidirus, said developing countries had agreed to give close attention to the strengthening of cybersecurity during the regional preparatory meeting for 2017 World Telecommunication Development Conference in Bali.

"Indonesia's proposal on follow-up discussions about cybersecurity issues has received wide support from developing countries. Cybersecurity is not on the International Telecommunication Union [ITU] agenda but we are striving to put it in its programs," he said as quoted by Antara after the closing of the meeting in Legian on Thursday.

The meeting aims to unite the common interests of countries in the Asia-Pacific. All aspirations will be brought to the World Telecommunication Development conference in Buenos Aires, Argentina, in October. Representatives of 29 ITU member countries from the Asia-Pacific attended the Bali meeting."

24.03.17

Computerworld New Zealand

Government wants more co-operation to improve cyber security

The New Zealand government has produced its first report into the implementation of its new cybersecurity strategy, in which it calls for greater cooperation with industry in order to fully realise its objectives.

"The government has released its first annual report on the implementation of its Cyber Security Strategy and its plans to address cyber crime, calling for government and the private sector to work together to drive improved cyber security across the economy.

The report follows release of the Cyber Security Strategy, Action Plan, and national plan to address cyber crime in December 2015. It sets out progress under the four goals of: achieving cyber resilience; building cyber capability; addressing cyber crime; and enhancing international cooperation."

27.03.17

Politico

NATO plans €3 billion investment in satellite bandwidth, cybersecurity

NATO have announced that it will spend €3billion on the development of satellite communications and cybersecurity within the alliance. The money will be put towards the defence of NATO outposts and to improve the existing standards amongst member states.

"As security threats move online, the NATO Communications and Information Agency wants to strengthen network capabilities.

To that end, the alliance plans to invest around €3 billion in satellite bandwidth and stronger cybersecurity, a NATO official confirmed today.

The contracts for the expansion will be presented in Ottawa, Canada's capital, at an April defense conference.

Advanced software to help coordinate across NATO forces will cost around €180 million, while €800 million will go to the alliance's air and missile defense infrastructure."

Privacy

28.03.17

SC Magazine

Microsoft president takes stand against turning over data

Microsoft President Brad Smith has stated in an interview that Microsoft will continue to retain customer data unless legally compelled by law enforcement to hand over data.

“Microsoft will continue its hard-line stance against handing over customer data to any government unless it is "legally compelled to," company President Brad Smith reiterated in an interview with a U.K. news outlet.

"We will not help any government, including our own, hack or attack any customer anywhere," Smith said in an interview Monday with the U.K.'s ITV News, advocating for strict limits to the data governments can obtain from private citizens.

In age when law enforcement is pushing for ever-increasing access to the private communications of citizens and corporations, in particular technology companies, Microsoft has said it wouldn't cave to demands from intelligence agencies to automatically provide access to the data of its users.”

Internet Inclusion

29.03.17

IT Web Africa

Facebook partners Kenyan SP to launch Express Wi-Fi

As part of a program to provide greater access to affordable public WiFi hotspots, Facebook has partnered with Kenyan ISP Surf to help launch its Express WiFi service.

“Facebook has partnered Kenyan internet service provider Surf to launch its Express Wi-Fi service, which will offer businesses in a variety of towns and cities access to a fast, affordable public Wi-Fi hotspot service.

Surf has already rolled out more than 100 Express Wi-Fi hotspots in several communities in the greater metropolitan area of Nairobi, and will this week launch the service in Kisumu and Mombasa.”

29.03.17

Digital Look

Avanti Communications to provide internet connectivity to Sub-Saharan Africa

Avanti Communications has announced that it will work with Governments and non-state actors in Sub-Saharan Africa to improve internet access in rural communities, through the use of its eco wi-fi technology.

"Shares in Avanti Communications surged on Wednesday on news that the satellite data provider has partnered with telecommunications firm Millicom to bring broadband connectivity to domestic consumers, businesses and governments in Sub-Saharan Africa.

The AIM-listed company will deploy its eco wi-fi technology across Sub-Saharan Africa to schools and communities in rural communities."

Global Institutions

23.03.17

IGP

Re-thinking ICANN's at large community

The ITEMS International consultancy have produced a draft report into the ICANN At-Large Advisory Committee, in which they find the body is not fit for its intended purpose. The draft report is now available for public comment.

"It's a simple message: the At-Large Advisory Committee isn't fit for purpose. That's the conclusion that external consultants ITEMS International have drawn in their draft report, now out for public comment, on the review of the ICANN At-Large community.

The 90-page report draws on face-to-face interviews with over 100 ICANN staff and community members and the results from a multilingual, global survey to conclude that At-Large is "excessively focused on internal, procedural matters" and is "perceived to be run by an unchanging group of individuals … who have struggled to make end-user input into policy advice processes a reality."

The report is less an explosive exposé and more a call to action – and some of the actions it calls for could make the problems it identifies worse."

24.03.17

ITU

Harnessing digital skills and mobile learning for inclusive sustainable development

This week saw the conclusion of the second ITU/UNESCO Policy Forum on Mobile Learning. The forum focused on how education in digital skills and the use of mobile technology can improve attainment of Sustainable Development Goals particularly amongst vulnerable groups.

"The second joint ITU/UNESCO Policy Forum on Mobile Learning was held in Paris, France on 24 March 2017.

The Policy Forum was jointly organized by the International Telecommunication Union (ITU) and the United Nations Educational Scientific and Cultural Organization (UNESCO) in collaboration with the United Nations Refugee Agency (UNHCR)."

24.03.17

ICANN

Successful Candidates Announced for ICANN59 Fellowship

ICANN has announced the 55 individuals selected to participate in the fellowship program accompanying the 59th Public Meeting in Johannesburg later this year. The chosen participants come from varying backgrounds, from end user groups, to academia and the government.

"ICANN announces 55 individuals from 43 countries selected to participate in ICANN's Fellowship program at the 59th Public Meeting in Johannesburg, South Africa from 26-29 June 2017. As ICANN59 is a Policy Forum, only alumni of the Fellowship Program were eligible to apply. These successful candidates represent all sectors of society including; civil, government, ccTLD operations, academia, facets of the business community, technical, security and end user groups."

27.03.17

Politico

NATO plans €3 billion investment in satellite bandwidth, cybersecurity

NATO have announced that it will spend €3billion on the development of satellite communications and cybersecurity within the alliance. The money will be put towards the defence of NATO outposts and to improve the existing standards amongst member states.

"As security threats move online, the NATO Communications and Information Agency wants to strengthen network capabilities.

To that end, the alliance plans to invest around €3 billion in satellite bandwidth and stronger cybersecurity, a NATO official confirmed today.

The contracts for the expansion will be presented in Ottawa, Canada's capital, at an April defense conference.

Advanced software to help coordinate across NATO forces will cost around €180 million, while €800 million will go to the alliance's air and missile defense infrastructure."

Diary Dates

Building the European data economy – 10.01.17-26.04.17

ENISA evaluation and review – 18.01.17 – 12.04.17

Open from 18 January to 12 April 2017.

ITU Council 2017 – 15.05.17 – 25.05.17

Geneva, Switzerland

Africa Internet Summit (AIS) 2017 – 29.05.17 – 02.06.17

Nairobi, Kenya

European Dialogue on Internet Governance – 06.06.17-07.06.17

Tallinn, Estonia

World Summit on the Information Society Forum (WSIS) 2017 – 12.06.17 – 16.06.17

Geneva, Switzerland

16th European Conference on Cyber Warfare and Security ECCWS – 29.06.17-30.06.17

Dublin, Ireland

ITU WTDC-17 – 09.10.17 – 20.10.17

Buenos Aires, Argentina

IGF 2017 – 18.12.17 – 21.10.17

Geneva, Switzerland