IEEE

interel
COUNT ON US

IEEE GLOBAL INTERNET POLICY MONITOR

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

20 December 2017

Synopsis

Scroll to read full summaries with links to news articles.

The **EU** has created a new security body named **PESCO** for its members, excluding **Malta**, **Denmark** and the **UK**, as an alternative to **NATO** resources. The body will allow member states to collaborate on matters of defence and **cybersecurity**.

A **German Court** has ruled that the country's **Foreign Intelligence Agency** (BND) does not have the authority to collect and store the **metadata** of international calls for **intelligence** purposes.

The **Federal Communications Commission** has voted by a margin of three to two to repeal **net neutrality** rules introduced under the Obama administration.

Republican Congresswoman **Marsha Blackburn** has introduced the **Open Internet Preservation Act** to replace certain **net neutrality** rules that were repealed by the **Federal Communications Commission**. Supporters of net neutrality say the legislation falls short of previous protections.

President Trump has published a new **National Security Strategy** which stats that **cyber attacks** will result in "swift and costly consequences" for foreign Governments, criminals and actors.

Chinese regulators have told **Google** and **Facebook** at a conference in **Geneva** that if they want access to China's 751 million users then they have to abide by the country's stringent **online laws**.

South Korean researchers have report that hackers supported by the **North Korean Government** have gained millions of dollars in **crypto-currencies** such as **Bitcoin**, as international sanctions have led hackers to seek alternative ways to raise finances.

TRAI, **India's** telecommunications regulator has stated its support for **net neutrality**, arguing that the principle is key to a free and open internet. These comments were made in response to the decision of the US regulator the **FCC** to end existing net neutrality rules.

The **European Union** is aiming to strike a deal with **Japan** to allow data to flow seamlessly between the bloc and Japan by early next year.

The **Ethiopian Government** has partially blocked **social media** platforms such as **Facebook**, **Twitter** and **YouTube** due to a rise in ethnic tensions and anti-Government **protests.**

The **Ericsson Mobility Report** has found that **Nigeria** and other sub-Saharan **African countries** will have **5G** subscriptions by 2022.

UK Air Chief **Marshall Peach** chair of the **NATO** military committee has warned that **Russia** could cut off **internet** communications to the UK and NATO nations after Russian ships were spotted close to underwater cables in the Atlantic.

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

21 December 2017

Table of Contents

Europe

Internet governance

15.12.17

Reuters

After U.S. decision, France says will continue to defend net neutrality

French Foreign Minister Jean-Yves Le Drian has said that France will continue to support net neutrality regardless of the US decision to dismantle US regulations

“France will continue to defend “net neutrality” irrespective of what other countries may do, Foreign Minister Jean-Yves Le Drian said on Friday, after a United States commission voted to ditch rules on the issue.”

“The U.S. Federal Communications Commission voted on Thursday to repeal the landmark 2015 rules aimed at ensuring a free and open internet, setting up a court fight over a move that could recast the digital landscape.”

18.12.17

Financial Times

Europe gears up to play pivotal role in ‘internet of things’

Carlos Moedas, the EU’s science and research chief has said that European companies have been slow to harness the app-based digital economy, however he believes the bloc will thrive in the ‘third wave’ of the digital transformation.

“As Europe’s economy recovers, companies and investors across the continent are gearing up for new opportunities, taking advantage of its hidden strengths: education, skills and innovative people. Here we look at plans by the EU’s science and research chief to ensure European companies thrive in the internet’s “third wave”’

“Europe’s expertise in engineering and science should enable it to dominate the “internet of things”, according to the EU’s science and research chief. But Carlos Moedas admits the bloc’s companies were slow to grasp the rise of the app-based digital economy.”

19.12.17

Reuters

Italian budget commission approves web tax on digital services

The Italian Government have approved a three percent levy on certain internet transactions in a bid to stop larger firms such as Google, Amazon and Apple benefitting from EU tax rules.

“The budget commission of Italy’s lower house approved on Tuesday a measure obliging companies to pay a 3 percent levy on some internet transactions in a move aimed at bypassing EU tax rules that benefit large tech firms.”

“The European Commission said it understood concerns over existing regulations, but urged member states to wait for Brussels to come up with an EU-wide solution to the problem rather than go it alone with separate legislation.”

20.12.17

Times

Tech bosses condemned for failure to delete hate posts

Addressing the Home Affairs Select Committee, Yvette Cooper, the Chairwoman, condemned Twitter, Facebook and YouTube for failing to remove racist and hate filled posts.

“MPs have criticised Twitter, Facebook and YouTube for failing to remove hate-filled posts that were flagged months ago and said they were complicit in grooming and radicalising people by recommending similar posts and accounts to their users.”

“At a hearing of the home affairs select committee, Yvette Cooper, the chairwoman, said Twitter had failed to remove anti-Semitic posts that were cited at a previous session in March. These include a tweet reading “high-speed picture of a filthy Jew getting bitch-slapped” that Nick Pickles, a Twitter executive, admitted was unacceptable.”

Cybersecurity

12.12.17

European Commission

Twelfth progress report towards an effective and genuine Security Union

The European Commission has published its 12th Security Union report which commends several cyber resilient initiatives that have stopped terrorists.

“*This is the twelfth monthly report on the progress made towards building an effective and genuine Security Union and covers developments under two main pillars: tackling terrorism and organised crime and the means that support them; and strengthening our defences and building resilience against those threats.”*

“It is almost a year since the 19 December 2016 Berlin Christmas market attack which left twelve dead and fifty-six injured and was perpetrated by an individual who used multiple identities to evade border and law enforcement authorities.”

13.12.17

European Parliament

MEPs advocate stronger EU foreign and defence policy

MEP’s have urged for closer EU defence ties to deal with irregular and cyber warfare threats from Russia.

“The EU’s foreign and defence policy should proceed with closer EU defence ties and a strong response to international threats, said MEPs on Wednesday.”

“MEPs welcome the fact that, following their repeated appeals, EU defence integration is getting under way with the launch of a European Defence Fund, an EU operational headquarters, a Permanent Structured Cooperation and an annual review of member states’ defence plans.”

14.12.17

Guardian

Russia could cut off internet to Nato countries, British military chief warns

UK Air Chief Marshall Peach chair of the NATO military committee has warned that Russia could cut off internet communications to the UK and NATO nations after Russian ships were spotted close to underwater cables in the Atlantic.

*“*Russia *could pose a major threat to the UK and other Nato nations by cutting underwater cables essential for international commerce and the internet, the chief of the British defence staff, Sir Stuart Peach, has warned.”*

“Russian ships have been regularly spotted close to the Atlantic cables that carry communications between the US and Europe *and elsewhere around the world.”*

15.12.17

SC Media

Europe creates new security body separate from NATO - UK not included

The EU has created a new security body named PESCO for its members, excluding Malta, Denmark and the UK, as an alternative to NATO resources. The body will allow member states to collaborate on matters of defence and cybersecurity.

“To be known as PESCO, the body will allow member states to jointly develop military capabilities, invest in shared projects and enhance their respective armed forces.”

“In response to major challenges threatening the EU's security, particularly hybrid and information warfare, proliferation of weapons of mass destruction, terrorism, conflicts in the Eastern and Southern neighbourhood as well as proxy wars the European Council this week agreed the creation of a new European defence and security cooperation network.”

19.12.17

GOV.UK

The National Security Strategy Committee

Mark Sedwill, Britain’s National Security Advisor, has addressed members of Parliament’s National Security Strategy Committee, where he warned that Cyber-attacks on undersea internet cables and computer networks would be greater than the World War 2’s Blitz.

“The Chair: Thank you very much for coming. As you probably know, we were a little dismayed that it took a while to set up the Committee, but we are grateful to you for coming so early in the period since we have been set up. We have all taken note of the fact that the Prime Minister has tasked you with reforms to the National Security Council process. What exactly are you considering?”

“Mr Mark Sedwill: Thank you, Madam Chair, and thank you very much for your welcome to this session. Essentially, there is a continuous process of trying to improve the operation of the National Security Council.”

21.12.17

Telegraph

GCHQ: British cyberweapons could paralyse hostile states

Britain has developed sophisticated cyberweapons capable of crippling a hostile state, GCHQ has revealed, amid warnings that Russia is launching more aggressive online attacks.

"Britain has developed sophisticated cyberweapons capable of crippling a hostile state, GCHQ has revealed amid warnings that Russia is launching more aggressive online attacks."

"Assaults on US central command, Twitter accounts and a French TV network, made to look like Islamist attacks, appear to have been Russia "ostentatiously flexing its muscles towards the West", parliament's intelligence and security committee (ISC) has been told."

Privacy

14.12.17

Reuters

German court rules against foreign intelligence mass communication surveillance

A German Court has ruled that the country's Foreign Intelligence Agency (BND) does not have the authority to collect and store the metadata of international calls for intelligence purposes.

"Germany's foreign intelligence agency (BND) must not store the metadata - such as phone numbers - of international phone calls for the purpose of intelligence analysis, a court rules on Thursday."

"Media freedom organization Reporters Without Borders filed a lawsuit in June 2015 against the BND, saying it had breached the organization's secrecy and harmed the partners and reporters it worked with."

15.12.17

Reuters

EU sees data transfer deal with Japan early next year

The European Union is aiming to strike a deal with Japan to allow data to flow seamlessly between the country and the EU by early next year.

"The European Union aims to conclude a deal allowing businesses to seamlessly transfer personal data between the bloc and Japan by early next year, building on the recent agreement on a free trade pact."

"Cross-border data flows are key to most businesses. These can include moving employee information around, credit card details to complete online transactions, and people's browsing habits to serve them targeted ads."

18.12.17

Reuters

French privacy watchdog raps WhatsApp over Facebook data sharing

France's privacy watchdog has criticised WhatsApp for wrongly sharing user data with Facebook without user's consent. The watchdog has threatened to fine the messaging app if it continuously fails to comply with French privacy law.

"France's data privacy watchdog may fine messaging app WhatsApp if it does not comply with an order to bring its sharing of user data with parent company Facebook into line with French privacy law."

"The French data protection authority - CNIL - said on Monday it had told WhatsApp to comply with the order within one month, and pay particular attention to obtaining users' consent. If WhatsApp does not comply it could sanction the company, it said."

Internet Inclusion

15.12.17

Ofcom

Connected Nations 2017

The UK's telecoms regulator Ofcom has published their annual report on broadband connection in the UK, which indicates that Scotland and Wales have returned the largest year-on year increase in superfast broadband coverage.

"This report outlines the main developments in coverage and performance of fixed broadband and mobile networks, as well as network security and resilience. Alongside this report, we have published reports summarising the findings for the four UK nations."

"We have also updated our mobile coverage checker app for smartphones and tablets, and our online visualisation tool, to help people find out more about the availability of fixed broadband and mobile services."

19.12.17

Department for Digital, Culture Media and Sport

Next Generation Mobile Technologies: An update to the 5G strategy for the UK

The UK's Department for Digital Culture Media and Sport have published a new 5G strategy which indicates the desire for greater infrastructure sharing and more 5G pilots.

"As we set out in the Digital Strategy, we are determined that the UK is a world leader in 5G so that we can take early advantage of the benefits that this new technology offers."

"Development of the next generation of digital communications in the UK continues at pace, and the path to 5G is becoming clearer. Since we published our 5G strategy in March, our understanding of the issues and challenges has increased. Now is the right time to update on our progress."

20.12.17

GOV.UK

High speed broadband to become a legal right

The UK Government have announced that high speed broadband will become a legal right to anyone that requests it, from 2020, with the introduction of a Universal Service Obligation of 10Mbps.

The Government has confirmed that universal high-speed broadband will be delivered by a regulatory Universal Service Obligation (USO), giving everyone in the UK access to speeds of at least 10 Mbps by 2020.

This is the speed that Ofcom, the independent regulator, says is needed to meet the requirements of an average family. After careful consideration the government has decided that regulation is the best way of making sure everyone in the UK can get a decent broadband connection of at least 10 Mbps as soon as possible.

United States of America

Internet governance

15.12.17

Guardian

US regulator scraps net neutrality rules that protect open internet

The Federal Communications Commission has voted by a margin of three to two to repeal net neutrality rules introduced under the Obama administration.

"The US's top media regulator voted to end rules protecting an open internet on Thursday, a move critics warn will hand control of the future of the web to cable and telecoms companies."

"At a packed meeting of the Federal Communications Commission (FCC) in Washington, the watchdog's commissioners voted three to two to dismantle the "net neutrality" rules that prevent internet service providers (ISPs) from charging websites more for delivering certain services or blocking others should they, for example, compete with services the cable company also offers."

18.12.17

Reuters

Internet giants told: Accept cyber curbs to be welcome in China

Chinese regulators have told Google and Facebook at a conference in Geneva that if they want access to China's 751 million users then they have to abide by its stringent online laws.

"Google and Facebook will have to accept China's censorship and tough online laws if they want access to its 751 million internet users, Chinese regulators told a conference in Geneva on Monday."

"That's a question maybe in many people's minds, why Google, why Facebook are not yet working and operating in China," said Qi Xiaoxia, director general of the Bureau of International Cooperation at the Cyberspace Administration of China (CAC)."

18.12.17

Reuters

Kaspersky Lab asks court to overturn U.S. government software ban

Moscow based Kaspersky Lab has urged the US federal court to overturn the Government's decision to ban Kaspersky products in Federal departments and agencies.

"*Moscow-based security software maker Kaspersky Lab said on Monday it has asked a U.S. federal court to overturn a Trump administration ban on use of its products in government networks, saying the move deprived the company of due process."*

"The Department of Homeland Security (DHS) in September issued a directive ordering civilian government agencies to remove Kaspersky software from their networks within 90 days. It came amid mounting concern among U.S. officials that the software could enable Russian espionage and threaten national security."

18.12.17

The White House

National Security Strategy

President Trump has published a new National Security Strategy which stats that cyber attacks will result in "swift and costly consequences" for foreign Governments, criminals and actors.

"The American people elected me to make America great again. I promised that my Administration would put the safe-, interests, and well-being of our citizens first. I pledged that we would revitalize the American economy, rebuild our military, defend our borders, protect our sovereignty, and advance our values."

"During my first year in office, you have witnessed my America First foreign policy in action. We are prioritizing the interests of our citizens and protecting our sovereign rights as a nation. America is leading again on the world stage. We are not hiding from the challenges we face. We are confronting them head-on and pursuing opportunities to promote the securi- and prosperi- of all Americans."

19.12.17

The Hill

[House Republican offers net neutrality replacement bill]

Republican Congresswoman Marsha Blackburn has introduced the Open Internet Preservation Act to replace certain net neutrality rules that were repealed by the Federal Communications Commission. Supporters of net neutrality say the legislation falls short of previous protections.

"Rep. Marsha Blackburn (R-Tenn.) on Tuesday introduced a bill that would replace some of the net neutrality rules that the Federal Communications Commission (FCC) repealed last week, though critics say that the legislation falls short of the previous protections."

"Blackburn's bill would prohibit internet service providers from blocking or throttling web content. But it would still allow companies such as Verizon and Comcast to charge websites for faster data speeds, and it pre-empts states from implementing stronger net neutrality protections."

Cybersecurity

19.12.17

Reuters

[U.S. blames North Korea for 'WannaCry' cyber attack]

The United States has officially blamed North Korea for the WannaCry cyber attack which crippled banks, hospitals and companies across the world.

"The Trump administration has publicly blamed North Korea for unleashing the so-called WannaCry cyber-attack that crippled hospitals, banks and other companies across the globe earlier this year."

"The attack was widespread and cost billions, and North Korea is directly responsible," Tom Bossert, homeland security adviser to President Donald Trump, wrote in a piece published on Monday night in the Wall Street Journal."

Privacy

19.12.17

SC Media

Backdoor ships SMS data back to China

A US based cybersecurity firm, Kryptowire has discovered that a Chinese company called Adups has been collecting SMS messages, call history, address books and sending this data to servers in China.

"A firmware code created by a Chinese company called Adups has been found to be collecting vasts amount of user information and sending it to servers located in China according to US cyber-security firm Kryptowire.

Kryptowire says that the backdoor code was collecting SMS messages, call history, address books, app lists, phone hardware identifiers, but it was also capable of installing new apps or updating existing ones. The backdoor code was hidden in a built-in and unremovable app, which was the component responsible for the firmware-over-the-air update (FOTA) system."

Internet Inclusion

No new items of relevance

Pan-Asia

Internet governance

13.12.17

China Daily

China now a leading global force in digital economy: Experts

A report by McKinsey Global Institute has found that China has become a major player in digital technology and continues to have massive potential for growth.

“China's digital transformation is likely to have an increasing influence on the worldwide digital landscape, considering the profound impact it is already having on its own economy, experts said here late Monday.”

"China is already a global digital economy and it is going to have a greater impact on the global digital world," Jonathan Woetzel, senior partner at Mckinsey and director of the McKinsey Global Institute (MGI), told Xinhua in a recent interview.”

15.12.17

The Economic Times

Keeping internet open right way forward for India: TRAI

TRAI, India’s telecommunications regulator has stated its support for net neutrality, arguing that the principle is key to a free and open internet. These comments were made in response to the decision of the US regulator the FCC to end existing net neutrality rules.

“Telecom regulator TRAI today strongly defended its stance on net neutrality, asserting that keeping the internet open and free is the "right way" forward for India.”

“The comments come in the backdrop of US regulator yesterday rolling back net neutrality regulations adopted by the Obama administration.”

18.12.17

Reuters

[Internet giants told: Accept cyber curbs to be welcome in China]

Chinese regulators have told Google and Facebook at a conference in Geneva that if they want access to China's 751 million users then they have to abide by the country's stringent online laws.

"Google and Facebook will have to accept China's censorship and tough online laws if they want access to its 751 million internet users, Chinese regulators told a conference in Geneva on Monday."

"That's a question maybe in many people's minds, why Google, why Facebook are not yet working and operating in China," said Qi Xiaoxia, director general of the Bureau of International Cooperation at the Cyberspace Administration of China (CAC)."

19.12.17

Reuters

[Bitcoin warnings grow more strident as Singapore urges 'extreme caution']

Singapore's central bank has warned the public to be extremely cautious about buying cryptocurrencies after a week of unstable trading that has raised concern that the currency is in a speculation bubble.

"Global financial regulators are beginning to warn the public against the risks of investing in a market that many feel is in a speculative bubble, with Singapore's central bank on Tuesday urging "extreme caution" about buying cryptocurrencies."

"The staggering growth of bitcoin and other decentralised digital currencies this year - with the market swelling from around $17 billion at the start of January to well over $600 billion now - has led to increasing concerns over what the fallout could be if the bubble were to suddenly burst."

19.12.17

Japan Today

[Bitcoin not yet proven as credible currency: Japan finance minister]

The Japanese Finance Minister Taro Aso has said that Bitcoin has, "not yet been proven to be credible enough to become a currency."

"Japanese Finance Minister Taro Aso said on Tuesday that bitcoin has not been proven to be a credible currency and that he would watch its developments in the near-term."

"He made the remark to reporters when asked about his French counterpart's comment this week that France would propose a discussion on regulating the virtual currency at a meeting of G20 group of major economies next year."

20.12.17

Economic Times (India)

Trai to meet telcos early Jan to discuss 2018 roadmap

TRAI, India's telecoms regulator will meet with telecommunication companies in early January to seek their views on TRAI's strategic priorities for 2018.

"The telecom regulator will seek views of all carriers to narrow down on some areas of priority that it should look into in 2018, for which it will meet the companies in the first week of January, chairman RS Sharma has said."

"The Telecom Regulatory Authority of India (Trai) will also begin drive tests for measuring quality of data services on a granular level, and is considering adding the option of viewing speeds of all networks at one's location or travel route in the MySpeed App, with the option for the consumer to choose that network. Both services will be greatly beneficial for consumers that typically face issues of call drops and inadequate data coverage in some instances."

Cybersecurity

14.12.17

Security Brief Asia

Singapore MINDEF opens doors to white hat hackers

David Koh the cyber chief for the Singapore Ministry of Defence has urged security experts to hack into the Government's defence systems in a bid to improve the departments cyber resilience.

"The Singapore Ministry of Defence (MINDEF) cyber chief David Koh is asking budding security experts to hack MINDEF systems – all with the aim of improving defences against the malicious hackers."

"Koh, who is also chief of the Cyber Security Agency of Singapore (CSA), announced the MINDEF Bug Bounty Programme this week. The announcement

comes off the back of his visit to the Cyber Defence Test and Evaluation Centre (CyTEC) on Tuesday."

19.12.17

Reuters

U.S. blames North Korea for 'WannaCry' cyber attack

The United States has officially blamed North Korea for the WannaCry cyber attack which crippled banks, hospitals and companies across the world.

"The Trump administration has publicly blamed North Korea for unleashing the so-called WannaCry cyber-attack that crippled hospitals, banks and other companies across the globe earlier this year."

"The attack was widespread and cost billions, and North Korea is directly responsible," Tom Bossert, homeland security adviser to President Donald Trump, wrote in a piece published on Monday night in the Wall Street Journal."

19.12.17

Reuters

Multi-stage cyber-attacks net North Korea millions in virtual currencies: researchers

South Korean researchers have report that hackers supported by the North Korean Government have gained millions of dollars in crypto-currencies such as Bitcoin, as international sanctions have led hackers to seek alternative ways to raise finances.

"A series of recent cyber-attacks has netted North Korean hackers millions of dollars in virtual currencies like bitcoin, with more attacks expected as international sanctions drive the country to seek new sources of cash, researchers say."

"North Korea's government-backed hackers have been blamed for a rising number of cyber-attacks, including the so-called WannaCry cyber-attack that crippled hospitals, banks and other companies across the globe this year."

20.12.17

Newshub

New Zealand spy agency 'concerned' by North Korean cyber attacks

The Director-General of the Government Communications Security Bureau Andrew Hampton has said that New Zealand was not safe after revelations that North Korea was behind the 'WannaCry' cyber-attack.

"A government spy agency warns it is "concerned" by revelations linking North Korea to the 'WannaCry' cyber-attack."

"Overseas intelligence agencies say that North Korea's Lazarus hacking group was behind the ransomware attack, which infected computers across the globe earlier this year."

Privacy

15.12.17

Reuters

EU sees data transfer deal with Japan early next year

The European Union is aiming to strike a deal with Japan to allow data to flow seamlessly between the bloc and Japan by early next year.

"The European Union aims to conclude a deal allowing businesses to seamlessly transfer personal data between the bloc and Japan by early next year, building on the recent agreement on a free trade pact."

"Cross-border data flows are key to most businesses. These can include moving employee information around, credit card details to complete online transactions, and people's browsing habits to serve them targeted ads."

19.12.17

SC Media

Backdoor ships SMS data back to China

A US based cybersecurity firm, Kryptowire has discovered that a Chinese company called Adups has been collecting SMS messages, call history, address books and sending this data to servers in China.

"A firmware code created by a Chinese company called Adups has been found to be collecting vasts amount of user information and sending it to servers located in China according to US cyber-security firm Kryptowire.

Kryptowire says that the backdoor code was collecting SMS messages, call history, address books, app lists, phone hardware identifiers, but it was also capable of installing new apps or updating existing ones. The backdoor code was hidden in a built-in and unremovable app, which was the component responsible for the firmware-over-the-air update (FOTA) system."

Internet Inclusion

13.12.17

China Daily

Bangladesh wants China as large partner to make digital dreams come true: Minister

Zunaid Ahmed Palak, State Minister for Bangladeshi Information and Communication Technology has said that he wants China to help build a digital Bangladesh by 2021.

"Bangladesh wants China to be its major partner to make the country's digital dreams come true, Bangladeshi Information and Communication Technology (ICT) State Minister Zunaid Ahmed Palak said."

"In an exclusive interview with Xinhua recently, the minister said, "For a long, long time we have been time-tested friends and in the field of ICT we are grateful to China and the Chinese government for helping us by providing all kinds of technical and financial support for building our infrastructure."

Rest of the World

Internet governance

18.12.17

IT News Africa

Ethiopian government blocks social media as violence spreads

The Ethiopian Government has partially blocked social media platforms such as Facebook, Twitter and YouTube due to a rise in ethnic tensions and anti-Government protests**.**

“*The Ethiopian government has partially blocked internet access in the country following the spread of violence across the country. According to a report by* Quartz*, citizens have been unable to reliably reach social media platforms such as Facebook, Twitter, and YouTube since Tuesday, 12 December 2017.”*

“There has been unrest in the East African country were clashes between different ethnic groups in the Oromiya region has claimed the lives of 61 people.”

18.12.17

Reuters

Kaspersky Lab asks court to overturn U.S. government software ban

Moscow based Kaspersky Lab has urged the US federal court to overturn the Government’s decision to ban Kaspersky products in Federal departments and agencies.

“*Moscow-based security software maker Kaspersky Lab said on Monday it has asked a U.S. federal court to overturn a Trump administration ban on use of its products in government networks, saying the move deprived the company of due process.”*

“The Department of Homeland Security (DHS) in September issued a directive ordering civilian government agencies to remove Kaspersky software from their networks within 90 days. It came amid mounting concern among U.S. officials that the software could enable Russian espionage and threaten national security.”

Cybersecurity

14.12.17

Guardian

Russia could cut off internet to Nato countries, British military chief warns

UK Air Chief Marshall Peach chair of the NATO military committee has warned that Russia could cut off internet communications to the UK and NATO nations after Russian ships were spotted close to underwater cables in the Atlantic.

*“*Russia *could pose a major threat to the UK and other Nato nations by cutting underwater cables essential for international commerce and the internet, the chief of the British defence staff, Sir Stuart Peach, has warned.”*

“Russian ships have been regularly spotted close to the Atlantic cables that carry communications between the US and Europe *and elsewhere around the world.”*

20.12.17

Newshub

New Zealand spy agency 'concerned' by North Korean cyber attacks

The Director-General of the Government Communications Security Bureau Andrew Hampton has said that New Zealand was not safe after revelations that North Korea was behind the ‘WannaCry’ cyber-attack.

“A government spy agency warns it is "concerned" by revelations linking North Korea to the 'WannaCry' cyber-attack.”

“Overseas intelligence agencies say that North Korea's Lazarus hacking group was behind the ransomware attack, which infected computers across the globe earlier this year.”

21.12.17

Telegraph

GCHQ: British cyberweapons could paralyse hostile states

Britain has developed sophisticated cyberweapons capable of crippling a hostile state, GCHQ has revealed amid warnings that Russia is launching more aggressive online attacks.

"Britain has developed sophisticated cyberweapons capable of crippling a hostile state, GCHQ has revealed amid warnings that Russia is launching more aggressive online attacks."

"Assaults on US central command, Twitter accounts and a French TV network, made to look like Islamist attacks, appear to have been Russia "ostentatiously flexing its muscles towards the West", parliament's intelligence and security committee (ISC) has been told."

Privacy

No new items of relevance

Internet Inclusion

14.12.17

IT News Africa

New reports highlight talent gaps that exist in Africa's Fintech landscape

The Digital Frontiers Institute based in Cape Town, South Africa, have published two reports which aim to help businesses reduce the human talent gaps in Africa's Fintech landscape.

"The Digital Frontiers Institute (DFI) has released two new reports *that aim to provide better understand and address human talent gaps that exist in Africa's Fintech landscape."*

"The 2017 Fintech Talent Africa Leadership and Employee Engagement Report and the 2017 Fintech Talent Africa Compensation Report provide data and insights for business leaders and entrepreneurs to help attract and retain the best people in Africa's increasingly competitive financial technology industry."

14.12.17

IT News Africa

BCX to invest $7.5 million into South African digital skills

BCX, Africa's leading premier ICT solutions and service provider has announced that it will invest $7.5 million to help close the digital skills gap in South Africa.

"On Thursday 14 December 2017, BCX announced that it will be investing $7.5 million (R100 million) to grow scarce digital skills in ICT infrastructure and

software programming alongside cybersecurity, Fintech and artificial intelligence over three years in partnership with the Cape Innovation and Technology Initiative (CiTi) in South Africa."

"The three-year project will be called CiTiX- Futured by BCX. In the project BCX and CiTi will train a minimum of 250 candidates each year in industry-led digital skills using CiTi's CapaCiTi programme skills development and job readiness methodology."

20.12.17

Guardian

Nigeria, other SSA countries to experience 5G by 2022

The Ericsson Mobility Report has found that Nigeria and other sub-Saharan African countries will have 5G subscriptions by 2022.

"With the International Telecommunications Union (ITU) targeting 2019 to standardise Fifth-Generation networks (5G), Ericsson Mobility Report, has predicted that Nigeria and other countries in sub-Saharan Africa will witness their first 5G subscriptions by 2022."

"The November edition of Ericsson Mobility Report revealed that the number of 5G subscriptions in SSA is expected to reach two million by 2023."

Global Institutions

14.12.17

Guardian

Russia could cut off internet to Nato countries, British military chief warns

UK Air Chief Marshall Peach chair of the NATO military committee has warned that Russia could cut off internet communications to the UK and NATO nations after Russian ships were spotted close to underwater cables in the Atlantic.

*“*Russia *could pose a major threat to the UK and other Nato nations by cutting underwater cables essential for international commerce and the internet, the chief of the British defence staff, Sir Stuart Peach, has warned.”*

“Russian ships have been regularly spotted close to the Atlantic cables that carry communications between the US and Europe *and elsewhere around the world.”*

15.12.17

SC Media

Europe creates new security body separate from Nato - UK not included

The EU has created a new security body named PESCO for its members, excluding Malta, Denmark and the UK, as an alternative to NATO resources. The body will allow member states to collaborate on matters of defence and cybersecurity.

“To be known as PESCO, the body will allow member states to jointly develop military capabilities, invest in shared projects and enhance their respective armed forces.”

“In response to major challenges threatening the EU's security, particularly hybrid and information warfare, proliferation of weapons of mass destruction, terrorism, conflicts in the Eastern and Southern neighbourhood as well as proxy wars the European Council this week agreed the creation of a new European defence and security cooperation network.”

Diary Dates

GDPR Summit – 30.01.18

London, England

Manusec Europe – 07.02.18-08.02.18

Munich, Germany

Global Internet and Jurisdiction Conference 2018 – 26.02.18-28.02.18

Ottawa, Canada

RSA – 16.04.18–20.04.18

San Francisco, USA

Africa Internet Summit – 29.04.18-11.05.18

Dakar, Senegal