29 November 2017

Synopsis

Scroll to read full summaries with links to news articles.

Foreign Ministers from across the **EU** have called for further resources and investment in **cybersecurity** as part of a recent **General Affairs Council** meeting.

Google is to be charged with breaching the **UK's Data Protection Act** after allegations emerged that the company has collected personal data from millions of **iPhone** users in the UK, tracking customers online behavior on the Safari browser.

A survey of 505 companies carried out by **Bitkom**, the German industry association for the information technology sector, has found that a quarter of **German companies** are worried that **digitalization** could threaten established companies.

US President **Donald Trump** has put **North Korea** back on the list of state sponsors of terrorism to facilitate greater powers to counter **cyber-attacks** from the country.

Military data belonging to the **US** Army Intelligence and Security Command has been found on an unsecured Amazon server. It exposed information about **project Red Disk**, a cloud-based intelligence platform.

Ajit Pai, Chairman of the **Federal Communications Commission** has accused **Twitter** of political **bias** while defending his plans for a roll back on **net neutrality**.

The **Chinese Government** has issued new **guidelines** and rules to regulate the country's **internet** finance sector. This crackdown has negatively affected US-listed Chinese financial firms.

TRAI, the Telecom Regulatory Authority of India has announced its recommendations for net neutrality. In 2016 TRAI ruled in favor of net neutrality, however these new regulations go further to prohibit any service provider from throttling data speeds.

In **Singapore**, credit and debit card **data** has been **stolen** once again from the **Uber** app, charging Singaporean citizens for 'phantom rides' often in overseas destinations.

The **South West African People's Organisation** has called for a **cybersecurity** ministry to be created in **Namibia** to, "control information" on social media and tackle **cybercrime**. However Swapo's proposals have been met with heavy criticism from **Access to Information** in Namibia.

New research has found that an increase in **internet access** in **Uganda** has also led to an increase in **cyber-attacks** in the country, as the Government has not developed a significant **cybersecurity** strategy.

The **International Telecommunications Union (ITU)** has announced that it will be creating an **Africa Regional Cybersecurity Centre** in **Abuja**, in conjunction with the **Nigerian Communications Commission**.

NATO has reported that it will expand its **cyber capabilities** to ensure it remains cyber resilient amongst the backdrop of growing threats from **Russia**. NATO said it must remain 'vigilant' in the cyber domain.

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

29 November 2017

Table of Contents

Europe

Internet governance

29.11.17

Computer Weekly

DCMS to spearhead review of UK telecoms sector

The Department for Digital, Culture, Media and Sport (DCMS) is set to review the UK's telecoms market, the aim is to create a strategy to increase the quality of infrastructure.

"The government is to embark on a landmark review of the UK's telecoms markets to investigate how it can better support investment in future connectivity."

"The Department for Digital, Culture, Media and Sport (DCMS) is to lead a major review of the UK's telecoms market with a view to investigating how it can best support investment in future connectivity standards."

Cybersecurity

21.11.17

Reuters

Denmark to ramp up cyber security efforts - defence minister

Denmark's Defence department has announced that more money will be invested into cybersecurity, as part of a new strategy to be published at the start of 2018.

"Denmark intends to invest to boost efforts to prevent cyber-attacks in a strategy to be presented early next year, its defence minister said on Tuesday."

"We are going to spend more money in this area," Claus Hjort Frederiksen told Reuters on the side-lines of a conference in Copenhagen, though he declined to disclose a figure.

23.11.17

The Portugal News

EU beefs up cybersecurity

Foreign Ministers from across the EU have called for further resources and investment in cybersecurity as part of a recent General Affairs Council meeting.

"The General Affairs Council has this week adopted conclusions calling for the strengthening of European cybersecurity and enhancing cyber resilience across the EU, in line with the tasking from the European Council in October 2017."

"The conclusions stress the need for all EU countries to make the necessary resources and investment available to address cybersecurity. They welcome the intention of increasing EU efforts in cybersecurity research and development by setting up a network of cybersecurity competence centres across the Union."

24.11.17

SC Media

Indian cyber-security event opened by PM, supported by UK

India's Prime minister, Narendra Modi delivered a speech at the Global Conference on Cyberspace in New Delhi. Lord Ahmad of Wimbledon, Minister of State for the Commonwealth and the UN said that the conference brought together those that have the power to keep the internet 'free, open and secure.'

"A demonstration of how seriously India is taking cyber-security is that the country's Prime Minister Narendra Modi delivered the keynote speech at the Global Conference on Cyberspace (GCCS) 2017 in New Delhi, India."

"A demonstration of how seriously India is taking cyber-security is that the country's Prime Minister Narendra Modi delivered the keynote speech at the Global Conference on Cyberspace (GCCS) 2017, held 23-24 November in New Delhi, India."

27.11.17

SC Media

Public sector digital defence spend up 3,183%: £20m on NHS cyber unit

Expenditure on digital defence in the UK has gone up by 3,183% this year, from £6 million of contracts secured last year to £191 million secured this year. The

NHS represents £20 million of that expenditure which it put toward a new cybersecurity unit.

"UK public sector expenditure on digital defences is up 3,183 percent this year - from £6 million of contracts tendered last year to £191 million tendered this year, according to Tussell, a government contracts analyst quoted in the Times newspaper today."

"Of that sum, £20 million is to be spent by the NHS on a new cyber-security unit - NHS Digital - which will use "ethical hackers" to look for weaknesses in the health service's defences. This makes the health service the third biggest public sector buyer of cyber-security."

28.11.17

Reuters

NATO sees growing Russia, China challenge; higher risk of war

NATO has reported that it will expand its cyber capabilities to ensure it remains cyber resilient amongst the backdrop of growing threats from Russia. NATO said it must remain 'vigilant' in the cyber domain.

"*China's growing military strength and a resurgent Russia will pose growing challenges to the trans-Atlantic alliance in coming years, and NATO's moves to bolster its capabilities could trigger a new Cold War-style arms race, a NATO report said."*

"The report, completed once every four years, identifies 20 global trends that are likely to affect the alliance through 2035, ranging from artificial intelligence and accelerating technology development to climate change and growing inequality."

29.11.17

Reuters

SWIFT warns banks on cyber heists as hack sophistication grows

SWIFT, the global banking messaging system has warned banks that digital heists are becoming more sophisticated. Their 16-page report outlined the new techniques hackers were using.

"SWIFT, the global messaging system used to move trillions of dollars each day, warned banks on Wednesday that the threat of digital heists is on the rise as hackers use increasingly sophisticated tools and techniques to launch new attacks."

"Brussels-based SWIFT has been urging banks to bolster security of computers used to transfer money since Bangladesh Bank lost $81 million in a February 2016 cyber heist that targeted central bank computers used to move funds. The new warning provided detail on some new techniques being used by the hackers."

Privacy

28.11.17

SC Media

UK public won't trust a breached company yet fail to protect their own data

A global Gemalto survey found that 70% of people said they would disassociate themselves with a company if it suffered a data breach. However, 27% of respondents feel that business take security seriously.

"70 percent of people say that they would stop doing business with companies following a data breach, but they are about to be engulfed in data breach reality with GDPR breach reporting as under-reporting of breaches is huge."

"The public are about to get a rude awakening when data breaches reported under GDPR become public as 70 percent of people say that they would stop doing business with companies following a data breach, yet it is clear within the industry that there is currently huge under-reporting of breaches."

30.11.17

Financial Times

Google faces UK suit over alleged snooping on iPhone users

Google is to be charged with breaching the UK's Data Protection Act after allegations emerged that the company has collected personal data from millions of iPhone users in the UK, tracking customers online behavior on the safari browser.

"Google illegally gathered the personal data of millions of iPhone users in the UK, according to a collective lawsuit led by a former director of the consumer group Which?"

"Richard Lloyd, a veteran consumer rights campaigner, alleges the technology company bypassed the default privacy setting on Apple phones and succeeded in tracking the online behavior of people using the safari browser."

Internet Inclusion

22.11.17

GOV.UK

Broadband Delivery UK

The Department for Culture, Media and Sport are delivering fibre broadband and full fibre networks to the whole of the UK.

“Broadband Delivery UK (BDUK), part of the Department for Culture, Media and Sport, is delivering superfast broadband and local full fibre networks to the nation.”

“The Government is supporting investment to provide superfast broadband coverage to 95% of the UK by December 2017. Provide access to basic broadband (2Mbps) for all. Stimulate private investment in full fiber connections by 2021.”

27.11.17

HM Government

Industrial Strategy: building a Britain fit for the future

In the Industrial Strategy fund, the Government announced that it would award £176 million for 5G and £200m for local areas to encourage roll out of fulfil fibre networks

“Over the last seven years, we have made huge progress in restoring our public finances and rescuing our economy from the brink of bankruptcy. Thanks to the sacrifices of the British people, the deficit is now down two-thirds since 2010, the unemployment rate is at its lowest in over 40 years and we have had 19 continuous quarters of economic growth.”

“We should take enormous pride in these achievements and the difference they are making for many families and businesses in our country. But at the same time, we must also recognise there are some communities which have struggled to keep pace with changes in the global economy and as a result not fully shared in the prosperity that growth has delivered.”

28.11.17

Reuters

Quarter of German firms see digital threat to survival

A survey of 505 companies carried out by Bitkom, the German industry association for the information technology sector, has found that a quarter of German companies are worried that digitalization could threaten established companies. They have urged the Government to make it a top priority.

"A quarter of German companies are worried that their survival is endangered by digitalization, while a large majority want the next German government to make the topic a priority, a survey showed on Tuesday."

"The survey of 505 companies conducted by Bitkom, the German industry association for the information technology sector, also showed that only 20 percent are investing in developing digital business models."

28.11.17

CSO

Cybersecurity skills shortage creating recruitment chaos

Companies and firms all over the world are facing a crisis of cybersecurity skills shortages. Recruitment is not doing much to fill these gaps, and with many people lacking such important skills companies face economic and business threats that they cannot handle.

"Because of the global cybersecurity skills shortage, nearly half of all cybersecurity professionals are solicited to consider other jobs at least once per week."

"Here's a quick review of some of the cybersecurity skills shortage data I've cited about in recent blogs: According to ESG research from early 2017, 45 percent of organizations claim to have a problematic shortage of cybersecurity skills."

United States of America

Internet governance

21.11.17

CNN Politics

Trump names North Korea a state sponsor of terrorism

US President Donald Trump has put North Korea back on the list of state sponsors of terrorism as part of a move to facilitate greater power to counter cyber-attacks from the country.

"President Donald Trump, in the latest demonstration of increased tensions on the Korean Peninsula, placed North Korea back on the list of state sponsors of terrorism."

"Trump announced the move Monday during a public meeting with his Cabinet at the White House and said the Treasury Department will announce new sanctions against North Korea on Tuesday."

21.11.17

SC Media

Two Democrats ask Appropriations Committee to give states $400M for election security

Rep. Bennie Thompson, D-Miss., and Rep. Robert Brady, D-Pa have asked the House Appropriations Committee for $400 million which is 'desperately needed' to secure elections and modernise voting technology.

"Two Democrats leading the Election Security Task Force have asked the House Appropriations Committee to carve out $400 million that is "desperately needed" to help states secure election systems and modernize their voting technology."

"We know that Russia launched an unprecedented assault on our elections in 2016, targeting 21 states' voting systems, and we believe this money is necessary to protect our elections from future attack," Rep. Bennie Thompson, D-Miss., and Rep. Robert Brady, D-Pa., wrote in a letter to the committee, noting that election meddling by a nation-state is akin to an attack on the U.S."

28.11.17

Reuters

FCC's Pai, addressing net neutrality rules, calls Twitter biased

Ajit Pai, Chairman of the Federal Communications commission has accused Twitter of political bias while defending his plans for a roll back on net neutrality. He said, “The company has a viewpoint and uses that viewpoint to discriminate.”

“The chairman of the Federal Communications Commission, Ajit Pai, accused social media company Twitter Inc (TWTR.N) of being politically biased on Tuesday as he defended his plan to roll back rules intended to ensure a free and open internet.”

“Pai, a Republican named by President Donald Trump to head up the FCC, unveiled plans last week to scrap the 2015 landmark net neutrality rules, moving to give broadband service providers sweeping power over what content consumers can access.”

30.11.17

The Guardian

US 'orchestrated' Russian spies scandal, says Kaspersky founder

Eugene Kaspersky, has accused the USA of creating the scandal impacting his company Kaspersky Labs. Mr Kaspersky believes the media coverage on the issue was the result of vast sums of money and lobbying as part of a “design” by the US Government.

“Eugene Kaspersky, chief executive and co-founder of the embattled Russian cybersecurity firm that bears his name, believes his company is at the center of a “designed and orchestrated attack” to destroy its reputation.”

“Over a short period in the summer of 2017, Kaspersky Labs was the subject of multiple media reports alleging that the company had helped Russian intelligence agencies spy on the US, a number of FBI raids on staff members, and a nationwide ban on the use of its software by federal government agencies.”

Cybersecurity

28.11.17

Reuters

NATO sees growing Russia, China challenge; higher risk of war

NATO has reported that it will expand its cyber capabilities to ensure it remains cyber resilient amongst the backdrop of growing threats from Russia. NATO said it must remain 'vigilant' in the cyber domain.

"*China's growing military strength and a resurgent Russia will pose growing challenges to the trans-Atlantic alliance in coming years, and NATO's moves to bolster its capabilities could trigger a new Cold War-style arms race, a NATO report said."*

"The report, completed once every four years, identifies 20 global trends that are likely to affect the alliance through 2035, ranging from artificial intelligence and accelerating technology development to climate change and growing inequality."

29.11.17

Reuters

SWIFT warns banks on cyber heists as hack sophistication grows

SWIFT, the global banking messaging system has warned banks that digital heists are becoming more sophisticated. Their 16-page report outlined the new techniques hackers were using.

"SWIFT, the global messaging system used to move trillions of dollars each day, warned banks on Wednesday that the threat of digital heists is on the rise as hackers use increasingly sophisticated tools and techniques to launch new attacks."

"Brussels-based SWIFT has been urging banks to bolster security of computers used to transfer money since Bangladesh Bank lost $81 million in a February 2016 cyber heist that targeted central bank computers used to move funds. The new warning provided detail on some new techniques being used by the hackers."

Privacy

28.11.17

SC Media

Wireless data tracking case to decide if US citizens have privacy rights

The US Supreme Court will soon decide whether a warrant needs to be obtained before accessing location data from wireless providers or invoke the 30-year-old stored Communications Act.

"An individual has no reasonable expectation of privacy in information voluntarily disclosed' is the premise being taken to the US Supreme Court Wednesday, to clarify if law enforcement must obtain warrants to access wireless data."

"When the US Supreme Court takes up Carpenter vs. the United States Wednesday, the likely landmark case will clarify if law enforcement must obtain court-issued warrants to access location data from wireless providers rather than invoke the lower standard for access imposed by the 30-year-old Stored Communications Act."

28.11.17

SC Media

UK public won't trust a breached company yet fail to protect their own data

A global Gemalto survey has found that 70% of people said they would disassociate themselves with a company if it suffered from data breach. However, 27% of respondents feel that business take security seriously.

"70 percent of people say that they would stop doing business with companies following a data breach, but they are about to be engulfed in data breach reality with GDPR breach reporting as under-reporting of breaches is huge."

"The public are about to get a rude awakening when data breaches reported under GDPR become public as 70 percent of people say that they would stop doing business with companies following a data breach, yet it is clear within the industry that there is currently huge under-reporting of breaches."

28.11.17

SC Media

Senators demand answers from Uber after breach debacle

US senators have demanded that Uber provides answers for the data breach incident that compromised the information of 57 million customers.

"U.S. senators on both sides of the aisle have sent letters to Uber demanding answers in the wake of the transportation company's disclosure that it concealed an October 2016 data breach incident that compromised the information of 57 million customers and drivers."

"Among the key questions posed by lawmakers to new Uber CEO Dara Khosrowshahi is why the company opted to pay hackers $100,000 to delete names, email addresses and other user data that they stole from an Amazon Web Services cloud database. Khosrowshahi revealed the breach incident on Nov. 22, roughly three months after taking over the chief executive role from Travis Kalanick, who was ousted following a series of corporate scandals. Although the company withheld news of the breach for a full year, Krosrowshahi claims he only recently learned of the attack."

28.11.17

SC Media

Unsecured AWS server exposed classified military intel

Military data belonging to the US Army Intelligence and Security Command has been found on an unsecured Amazon server. It exposed information about project Red Disk an Army cloud-based intelligence platform.

"Sensitive military data found on an unsecured Amazon server belonging to the U.S. Army Intelligence and Security Command (INSCOM), a joint Intelligence effort with the NSA, was accessible to the public and included information on project Red Disk, an Army cloud-based intelligence platform, an auxiliary to the Distributed Common Ground System (Army DCGS-A), that failed."

Internet Inclusion

No new items of relevance

Pan-Asia

Internet governance

21.11.17

CNN Politics

Trump names North Korea a state sponsor of terrorism

US President Donald Trump has put North Korea back on the list of state sponsors of terrorism as part of a move to facilitate greater power to counter cyber-attacks from the country.

"President Donald Trump, in the latest demonstration of increased tensions on the Korean Peninsula, placed North Korea back on the list of state sponsors of terrorism."

"Trump announced the move Monday during a public meeting with his Cabinet at the White House and said the Treasury Department will announce new sanctions against North Korea on Tuesday."

21.11.17

Reuters

China clamps down on online micro lending; U.S.-listed shares plunge

The Chinese Government has issued new guidelines and rules to regulate the internet finance sector. This crackdown has negatively affected US-listed Chinese financial firms by sending them into a 'tailspin.'

"China took steps to rein in the rapidly growing and lightly regulated market for online micro-lenders in the government's latest crackdown on internet finance, sending shares of U.S.-listed Chinese financial firms into a tailspin."

"A top-level Chinese government body issued an urgent notice on Tuesday to provincial governments urging them to suspend regulatory approval for the setting up of new internet micro-lenders, sources who had seen the notice told Reuters."

22.11.17

Time

[China Is Investigating its Former Internet Censor-in-Chief for Corruption]

Lu Wei, China's top internet regulator is being investigated by the communist party's anti corrupting for "serious violations of discipline." Mr. Wei had power over 700 million Chinese internet users and was a gatekeeper for technology companies wanting to do business with China.

"China's former top internet regulator and censor is being investigated by the ruling Communist Party's anti-corruption arm, the agency said Tuesday."

"The party's anti-graft watchdog agency said in a brief statement on its website that Lu Wei is suspected of "serious violations of discipline." Until Tuesday's announcement, Lu had been deputy head of the party's propaganda department."

28.11.17

Reuters

[Indian telecom regulator backs open internet]

TRAI, the Telecom Regulatory Authority of India has announced its recommendations for net neutrality. Back in 2016 TRAI ruled in favor of net neutrality, however these new regulations go further to prohibit any service provider from throttling data speeds.

"India's telecoms regulator made long-awaited recommendations on Tuesday to ensure an open internet and prevent any discrimination in internet access in the country."

"After more than a year of debate, the Telecom Regulatory Authority of India (TRAI) said it opposed any "discriminatory treatment" of data, including blocking, slowing or offering preferential speeds or treatment to any content."

28.11.17

Network Asia

[Cisco and INTERPOL join forces to combat cybercrime]

Cisco and INTERPOL, one of the largest policy organisations in Singapore have collaborated to develop a strong coordinated response to cyber-attacks.

"Cisco and INTERPOL, the world's largest international police organization, have agreed to share threat intelligence as the first step in jointly fighting cybercrime."

"Headed by INTERPOL's global cybercrime center, the INTERPOL Global Complex for Innovation (IGCI) in Singapore, the alliance will see the two organizations develop a coordinated and focused approach to data sharing. This not only will allow for quick threat detection around the world, but also pave the way for potential future collaboration on training and knowledge sharing."

Cybersecurity

24.11.17

SC Media

Indian cyber-security event opened by PM, supported by UK

India's Prime minister, Narendra Modi delivered a speech at the Global Conference on Cyberspace in New Delhi. Lord Ahmad Ahmad of Wimbledon, Minister of State for the Commonwealth and the UN said that the conference brought together those that have the power to keep the internet 'free, open and secure.'

"A demonstration of how seriously India is taking cyber-security is that the country's Prime Minister Narendra Modi delivered the keynote speech at the Global Conference on Cyberspace (GCCS) 2017 in New Delhi, India."

"A demonstration of how seriously India is taking cyber-security is that the country's Prime Minister Narendra Modi delivered the keynote speech at the Global Conference on Cyberspace (GCCS) 2017, held 23-24 November in New Delhi, India."

27.11.17

Reuters

Siemens, Trimble, Moody's breached by Chinese hackers, U.S. charges

The US Department of Justice have charged three Chinese nationals for hacking into Siemens, AG, Trimbnle Inc. and Moody's Analytics. The defendants were owners, employees and associates of the cyber security company, Guangzhou Bo Yu.

"U.S. prosecutors have charged three Chinese nationals affiliated with a cyber security company in China with hacking into Siemens AG, Trimble Inc and Moody's Analytics to steal business secrets."

"An indictment unsealed on Monday in federal court in Pittsburgh, Pennsylvania, charged the three with launching "coordinated and unauthorized" cyber attacks between 2011 and 2017."

28.11.17

Reuters

NATO sees growing Russia, China challenge; higher risk of war

NATO has reported that it will expand its cyber capabilities to ensure it remains cyber resilient amongst the backdrop of growing threats from Russia. NATO said it must remain 'vigilant' in the cyber domain.

"*China's growing military strength and a resurgent Russia will pose growing challenges to the trans-Atlantic alliance in coming years, and NATO's moves to bolster its capabilities could trigger a new Cold War-style arms race, a NATO report said."*

"The report, completed once every four years, identifies 20 global trends that are likely to affect the alliance through 2035, ranging from artificial intelligence and accelerating technology development to climate change and growing inequality."

29.11.17

Reuters

SWIFT warns banks on cyber heists as hack sophistication grows

SWIFT, the global banking messaging system has warned banks that digital heists are becoming more sophisticated. Their 16-page report outlined the new techniques hackers were using.

"SWIFT, the global messaging system used to move trillions of dollars each day, warned banks on Wednesday that the threat of digital heists is on the rise as hackers use increasingly sophisticated tools and techniques to launch new attacks."

"Brussels-based SWIFT has been urging banks to bolster security of computers used to transfer money since Bangladesh Bank lost $81 million in a February 2016 cyber heist that targeted central bank computers used to move funds. The new warning provided detail on some new techniques being used by the hackers."

Privacy

20.11.17

NewsAsia

Uber users in Singapore charged for 'phantom rides' overseas

In Singapore, credit and debit card data has been stolen once again from the Uber app, charging Singaporean citizens for 'phantom rides' that they never too, in often overseas destinations.

"Several Uber users in Singapore have complained this month of being charged for rides they never took, often in faraway places."

"The victims, who held credit or debit cards from different banks, were charged in foreign currencies including the US dollar, euro and British pound."

28.11.17

SC Media

UK public won't trust a breached company yet fail to protect their own data

A global Gemalto survey found that 70% of people said they would disassociate themselves with a company if it suffered from data breach. However, 27% of respondents feel that business take security seriously.

"70 percent of people say that they would stop doing business with companies following a data breach, but they are about to be engulfed in data breach reality with GDPR breach reporting as under-reporting of breaches is huge."

"The public are about to get a rude awakening when data breaches reported under GDPR become public as 70 percent of people say that they would stop doing business with companies following a data breach, yet it is clear within the industry that there is currently huge under-reporting of breaches."

Internet Inclusion

No new items of relevance

Rest of the World

Internet governance

24.11.17

The Herald

African Ministers of Communication and Information Technologies reiterate the need for Africa to become actively involved in the dynamics of "Internet Governance, Cybersecurity, and Cybercrime

A session held between a number of African Ministers on communication and technology again upheld the idea that the African Continent and all its nations need to increase their capability and involvement in cybersecurity and internet governance. The session discussed issues on potential regional and continental programmes to help enhance this.

"Since the previous session of the Special Technical Committee on Communication and ICT which took place in September 2015, notable developments have taken place in the sectors of communication and information technology and in the infrastructure development as general."

"It is against this backdrop among others that, African Ministers of Communication and Information Technologies gathering today in Addis Ababa in their second ordinary session of the Specialized Technical Committee on Communication and ICT (STC CICT-2) to discuss and make decisions on continental and regional programmes that impact Africans in the communications and ICT sectors."

30.11.17

The Guardian

US 'orchestrated' Russian spies scandal, says Kaspersky founder

Eugene Kaspersky, has accused the USA of creating the scandal impacting his company Kaspersky Labs. Mr Kaspersky believes the media coverage on the issue was the result of vast sums of money and lobbying as part of a "design" by the US Government.

"Eugene Kaspersky, chief executive and co-founder of the embattled Russian cybersecurity firm that bears his name, believes his company is at the center of a "designed and orchestrated attack" to destroy its reputation."

"Over a short period in the summer of 2017, Kaspersky Labs was the subject of multiple media reports alleging that the company had helped Russian

intelligence agencies spy on the US, a number of FBI raids on staff members, and a nationwide ban on the use of its software by federal government agencies."

Cybersecurity

23.11.17

New Vison

Uganda still regarded a high-risk nation for Cyber-attacks

An increase in internet access in Uganda has led to an increase in cyber-attacks in the country, as the Government has not developed a significant cybersecurity strategy.

"Cybercrime throughout Uganda is resulting in a loss of up to 122 billion Ugandan shillings for the nation according to a new Africa cybersecurity report for 2016, as compiled by Kenyan cybercrime organization, Serianu Cyber Threat Intelligence."

"Internet usage is growing rapidly in Uganda. Data from the United Nations Department of Economic and Social Affairs shows that just 0.1% of the population had internet access in 2000, but now almost a third (31.3%) of the Ugandan population are online, amounting to over 13 million web users. Consequently, the number of Ugandan cyber-criminals is rising thanks to the increasing sophistication of their knowledge while the lack of a cybercrime regulatory framework by the Ugandan authorities is creating huge loopholes for hackers to exploit online."

28.11.17

The Guardian (Nigeria)

West African cyber security summit holds March 21

Lagos will host the West African Cyber Security Summit in March 2018. The Summit aims to enhance knowledge, understanding and practice of technology and cyber threats to both governments and private companies.

"The West African Cyber Security Summit (WACSS) has been scheduled to take place on March 21, 2018 alongside Securex West Africa at the Landmark Centre in Lagos."

"The WACSS is the ultimate platform to learn about essential market developments, key trends, cutting-edge technology and to discuss strategies to address the latest risks and threats facing the industry."

28.11.17

IT News Africa

[Attivo Networks bolsters security defences across South and Sub-Saharan Africa with Networks Unlimited]

A large cybersecurity firm, Attivo Networks, will be working with Networks Unlimited, a value-added distributor, in order to secure better cyber defence on the African Continent. The partnership will aim to ensure better cybersecurity for the millions of people now using software and technology across Africa.

"Attivo Networks, the leader in deception for cyber security threat detection, on Tuesday 28 November 2017 announced a strategic partnership with Networks Unlimited, Africa's leading value-added distributor."

"With this distribution partnership, Attivo Networks and Networks Unlimited together aim to extend comprehensive next-generation deception-based cyber security defence to customers across the South and Sub-Saharan region."

28.11.17

Reuters

[NATO sees growing Russia, China challenge; higher risk of war]

NATO has reported that it will expand its cyber capabilities to ensure it remains cyber resilient amongst the backdrop of growing threats from Russia. NATO said it must remain 'vigilant' in the cyber domain.

"*China's growing military strength and a resurgent Russia will pose growing challenges to the trans-Atlantic alliance in coming years, and NATO's moves to bolster its capabilities could trigger a new Cold War-style arms race, a NATO report said."*

"The report, completed once every four years, identifies 20 global trends that are likely to affect the alliance through 2035, ranging from artificial intelligence and accelerating technology development to climate change and growing inequality."

29.11.17

Namibian

[Swapo eyes the creation of cyber security ministry]

The South West African People's Organisation has called for a cyber security ministry to be created in Namibia to, "control information" on social media and

tackle cybercrime. However Swapo's proposals have been met with heavy criticism from Access to Information in Namibia.

"A CYBER security ministry should be created to "control information" on social media, one of the resolutions of the recently concluded Swapo congress states."

"The proposed ministry would also be tasked with tackling cyber crime, including hacking and monitoring illicit [financial] flows."

29.11.17

Reuters

SWIFT warns banks on cyber heists as hack sophistication grows

SWIFT, the global banking messaging system has warned banks that digital heists are becoming more sophisticated. Their 16-page report outlined the new techniques hackers were using.

"SWIFT, the global messaging system used to move trillions of dollars each day, warned banks on Wednesday that the threat of digital heists is on the rise as hackers use increasingly sophisticated tools and techniques to launch new attacks."

"Brussels-based SWIFT has been urging banks to bolster security of computers used to transfer money since Bangladesh Bank lost $81 million in a February 2016 cyber heist that targeted central bank computers used to move funds. The new warning provided detail on some new techniques being used by the hackers."

Privacy

28.11.17

SC Media

UK public won't trust a breached company yet fail to protect their own data

A global Gemalto survey found that 70% of people said they would disassociate themselves with a company if it suffered from data breach. However, 27% of respondents feel that business take security seriously.

"70 percent of people say that they would stop doing business with companies following a data breach, but they are about to be engulfed in data breach reality with GDPR breach reporting as under-reporting of breaches is huge."

"The public are about to get a rude awakening when data breaches reported under GDPR become public as 70 percent of people say that they would stop

doing business with companies following a data breach, yet it is clear within the industry that there is currently huge under-reporting of breaches."

Internet Inclusion

29.11.17

Sundiata Post

NCC, ITU To Establish Africa Regional Cybersecurity Centre In Abuja

The International Telecommunications Union (ITU) has announced that it will be creating an Africa Regional Cybersecurity Centre in Abuja, in conjunction with the Nigerian Communications Commission.

"The Nigerian Communications Commission (NCC) said it is working with the International Telecommunications Union (ITU) to set up Africa Regional Cybersecurity Centre (RCC) in Abuja to deal with the increasing cybersecurity threats facing the continent."

"Executive Vice Chairman of NCC, Professor Umar Danbatta, at the official opening of the 27th African Information Network Centre (AFRINIC) in Lagos Tuesday, said the centre will be used for information sharing (cyber-attacks, threats, malware, viruses, etc) and also train African countries on cyber-related issues."

Global Institutions

28.11.17

Reuters

NATO sees growing Russia, China challenge; higher risk of war

NATO has reported that it will expand its cyber capabilities to ensure it remains cyber resilient amongst the backdrop of growing threats from Russia. NATO said it must remain 'vigilant' in the cyber domain.

"*China's growing military strength and a resurgent Russia will pose growing challenges to the trans-Atlantic alliance in coming years, and NATO's moves to bolster its capabilities could trigger a new Cold War-style arms race, a NATO report said."*

"The report, completed once every four years, identifies 20 global trends that are likely to affect the alliance through 2035, ranging from artificial intelligence and accelerating technology development to climate change and growing inequality."

29.11.17

Sundiata Post

NCC, ITU To Establish Africa Regional Cybersecurity Centre In Abuja

The International Telecommunications Union (ITU) has announced that it will be creating an Africa Regional Cybersecurity Centre in Abuja, in conjunction with the Nigerian Communications Commission.

"The Nigerian Communications Commission (NCC) said it is working with the International Telecommunications Union (ITU) to set up Africa Regional Cybersecurity Centre (RCC) in Abuja to deal with the increasing cybersecurity threats facing the continent."

"Executive Vice Chairman of NCC, Professor Umar Danbatta, at the official opening of the 27th African Information Network Centre (AFRINIC) in Lagos Tuesday, said the centre will be used for information sharing (cyber-attacks, threats, malware, viruses, etc) and also train African countries on cyber-related issues."

27.11.17

Council on Foreign Relations

How "Cyber" Sidelined "Development" at the ITU's World Telecommunication Development Conference

In this year's World Telecommunication Development Conference, held in Argentina by the ITU, cybersecurity and technology dwarfed any discussion about 'development' on social and economic issues. Despite it being the central focus, no agreement was made on cybersecurity and concerns and issues still pervade many nations across the world.

"Cybersecurity has made the World Telecommunication Development Conference another political battleground for digital policy, threatening to sideline the very real problems that developing countries need to solve."

"Every four years or so, the International Telecommunication Union (ITU) holds the World Telecommunication Development Conference (WTDC), and this year's conference was held in Buenos Aires, Argentina."

Diary Dates

IGF 2017 – 18.12.17–21.12.17

Geneva, Switzerland

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