13 December 2017

Synopsis

Scroll to read full summaries with links to news articles.

All **EU** member states except Malta, **Denmark** and the **UK** have signed up to work together on a set of 17 collaborative defence projects. One of these includes creating **cyber raid response** teams to deal with emerging threats.

The **European Commission** has intervened in an ongoing case between the **US Government** and **Microsoft** to ensure that the US Department of Justice correctly understands the EU's **data protection** laws.

European telecommunications ministers have agreed to the EU's roadmap for the development of the 5th generation **mobile networks**. The roadmap sets out the ambition of having **5G** in large cities and along transport routes in every European country by 2025.

Huawei, the **Chinese** tech giant has been banned from bidding on Government contracts in the **United States** over concerns that **Beijing** is using the equipment for **espionage**. In **Europe**, however, Huawei is set to deliver the next generation **5G network technology**.

The **US** President, **Donald Trump** has voiced his objection to a provision in the Defence Policy Bill which limits funding for the White House Communications Agency, "contingent upon the submission of a report on a national policy for **cyberspace**, **cybersecurity**, and **cyberwarfare**."

The **US Army** has launched a new programme with the aim of recruiting civilians with technology and **cybersecurity** skills, in a drastic attempt to strengthen the US cyber force.

A new **Artificial Intelligence Research Centre** will be opened in **China** by **Google**. The aim of developing **artificial intelligence** has been strongly supported by the Chinese Government but has largely restricted its use to state-owned companies.

The **Chinese Government** has announced its intention to create a national **cybersecurity** industrial park. The announcement comes as part of its plan to

enhance its **big data** strategy and contribute significantly to the Chinese economy.

Sergei Lavrov, Russia's Foreign Minister, has suggested that the **Organisation for Security and Cooperation in Europe** should increase its efforts on **internet safety**. The call from the Minister follows huge allegations by other nations of **Russia cyberattacks** and interference.

Liberia has suggested that, with help from more advanced nations, they can achieve great advancements in the technological and **cybersecurity** sector. The Foreign Minister, **Marjon Kamara**, believes that **internet and technology** will be key to the nations success in growing its economy.

As part of its aim of increasing **internet access** and **connectivity**, Kenya's mobile network operator, **Safaricom**, has revealed its intention to expand its **4G** network to all 47 counties in **Kenya**. The news comes just three years after 4G was rolled out in the country.

The Deputy Secretary of NATO, General **Rose Gottemoeller** has announced that **NATO** will help support **cyber technology** and security in the **Moldovan** education system by offering courses in universities.

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

13 December 2017

Table of Contents

Europe

Internet governance

11.12.17

Politico

[China's ghost in Europe's telecom machine](#)

Huawei, the Chinese tech giant has been banned from bidding on Government contracts in the United States over concerns that Beijing is using the equipment for espionage. In Europe, however, Huawei is set to deliver the next generation 5G network technology.

"Huawei has succeeded in Europe where it has failed in the United States — and that's becoming a problem on the Continent."

"The Chinese tech giant is banned from bidding for government contracts in the U.S. over concerns that its telecommunication equipment could be used for spying by Beijing."

Cybersecurity

07.12.17

Reuters

[Russia calls on OSCE states to ramp up cyber security efforts](#)

Sergei Lavrov, Russia's Foreign Minister, has suggested that the Organisation for Security and Cooperation in Europe should increase its efforts on internet safety. The call from the Minister follows huge allegations by other nations of Russia cyberattacks and interference.

"Russia's foreign minister called on Organization for Security and Cooperation in Europe (OSCE) countries to strengthen efforts to ensure the safety of the internet on Thursday.

"Moscow faces widespread allegations that it interfered in the U.S. presidential election and was behind a wave of destructive global hacking attacks. It has denied any involvement in either."

08.12.17

CrowdStrike

[2017 Cyber Intrusion Services Casebook](#)

CrowdStrike Researchers reported that malware-free or fileless attacks are on the rise as the lines between nation-state sponsored attacks and eCrime threat actors are blurred.

"Several key trends emerged from the incident response (IR) cases the CrowdStrike Services team handled on behalf of clients this past year. The team's case summaries and statistics show vividly how resourceful and relentless sophisticated attackers can be as they continually look for gaps in clients' IT infrastructure. Organizations should realize:"

"The lines between nation-state sponsored attack groups and eCrime threat actors continue to blur. Secondly, Self-propagation techniques have added a new twist to ransomware attacks and their ability to paralyze clients' operations."

08.12.17

NATO

[NATO and the European Union deepen cooperation on cyber defence](#)

European Union officials have met with their counterparts at NATO's Headquarters to discuss further cooperation on cyber defence.

"We reviewed our progress on enhancing information exchange, training and education, and exercises, while identifying new areas where more can be done – such as the sharing of best practice on crisis management and response," stated Dr. Jamie Shea, NATO's Deputy Assistant Secretary General for Emerging Security Challenges.

The officials discussed recent developments related to NATO's Cyber Defence Pledge and the implementation of NATO's decision to recognise cyberspace as a domain of operations, in addition to the new EU cybersecurity 'package'.

10.12.17

The Hill

[German spy chief warns of Chinese cyber infiltration effort](#)

Hans-Georg Maassen, the Head of Germany's domestic intelligence agency, Bfv has warned that Chinese intelligence agencies are hacking into networks and

targeting European businesses and officials. Maasen has stated that so far over 10,000 Germans have been affected.

"The head of Germany's domestic intelligence agency, BfV, said Sunday that Chinese intelligence agents are using LinkedIn to target European officials and businesses, The Associated Press reported Sunday."

"Hans-Georg Maassen said more than 10,000 Germans have been targeted by Chinese agents posing as consultants, headhunters or researchers, mainly through the professional networking site."

11.12.17

European Commission

[**European Commission welcomes first operational steps towards a European Defence Union**](#)

All EU member states except Malta, Denmark and the UK have signed up to work together on a set of 17 collaborative defence projects. One of these includes creating cyber raid response teams to deal with emerging threats.

"The European Commission welcomes the decision adopted today by the Council formally establishing Permanent Structured Cooperation (PESCO) and the plans presented by 25 EU Member States to work together on a first set of 17 collaborative defence projects."

"President Juncker said: "In June I said it was time to wake up the Sleeping Beauty of the Lisbon Treaty: permanent structured cooperation. Six months later, it is happening. I welcome the steps taken today by Member States to lay the foundations of a European Defence Union."

11.12.17

The Times

[**Cybersecurity is a challenge we must push up the political agenda**](#)

Michel Barnier, the EU's chief Brexit negotiator has confirmed that the UK will no longer be a member of Europol post-Brexit as of March 30, 2019, cutting the UK off from the organisation's cybersecurity support.

"Michel Barnier, the EU's chief Brexit negotiator, has announced that the UK will be no longer be a member of Europol once it leaves the EU."

"Yet the nature of modern-day organised crime knows no borders. The international nature of crime demonstrates the necessity of global cooperation to

ensure law enforcement is effective, not least in the area of cybercrime, which is a priority for Europol in its 2016-20 strategy cycle."

Privacy

08.12.17

SC Media

[**EC amicus brief in Microsoft Irish server case to school SCOTUS on data protection laws**](#)

The European Commission has intervened in an ongoing case between the US Government and Microsoft to ensure that the US Department of Justice correctly understands the EU's data protection laws.

"The European Commission has said it will file an amicus brief with the U.S. Supreme Court in the U.S. vs. Microsoft case on behalf of the European Union (EU)."

"Given that the transfer of personal data by Microsoft from the EU to the U.S. would fall under the EU data protection rules, the Commission considered it to be in the interest of the EU to make sure that EU data protection rules on international transfers are correctly understood and taken into account by the U.S. Supreme Court."

Internet Inclusion

07.12.17

Computer Weekly

[**EU telecoms ministers set out 5G mobile network roadmap**](#)

European telecommunications ministers have agreed to the EU's roadmap for the development of the 5th generation mobile networks. The roadmap sets out the ambition of having 5G in large cities and along transport routes in every European country by 2025.

"Telecommunications ministers from across Europe have agreed on a joint roadmap that will govern the deployment of 5G mobile networks across the EU"

"Telecoms ministers from around Europe have agreed on a European Union (EU) roadmap for the development of 5G mobile networks, establishing common ground on the harmonisation of radio spectrum bands and how they will be allocated to mobile network operators (MNOs), and thereby paving the way for mass deployment of 5G across the EU."

08.12.17

NATO

[Joint press point](#)

The Deputy Secretary of NATO, General Rose Gottemoeller has announced that NATO will help support cyber technology and security in the Moldovan education system by offering courses in universities.

"Welcome—the warmest welcome possible—to the opening of the brand-new NATO Liaison Office here in Chisinau. This is a moment of great pride for the NATO Alliance, and a clear sign of the importance that we place on our relationship with Moldova."

"Today is the culmination of almost 25 years of partnership between Moldova and NATO. The Liaison Office was built at the request of the Moldovan government to help drive our partnership, joining similar Liaison Offices in Kiev, Tbilisi, and Moscow."

08.12.17

Computer Weekly

[Code First Girls aims to teach 20,000 girls to code by 2020](#)

Code First, a social enterprise that offers free coding courses to girls, have launched a campaign to get 20,000 young women coding by 2020.

"Social enterprise Code First: Girls has launched a campaign with the aim of teaching 20,000 young women to code by 2020"

"Code First Girls has launched a campaign with the aim of teaching coding to 20,000 young women by 2020. The social enterprise has partnered with organisations KKR and OVH to provide employers with training support to teach the young women in their organisations to code, as well as provide free coding courses to women through other charitable institutions."

11.12.17

House of Commons Hansard

[Coding and Programming Education](#)

During a House of Commons debate, the Minister for School Standards, Nick Gibb has said that the UK Government will commit £84 million in new funding between 2018 and 2023 to support computing teaching in schools.

"We are committing £84 million of new funding between 2018 and 2023 to support computing teaching in schools, which will include training up to 8,000 secondary teachers to teach the new computing science GSCE, a national centre for computing education and an online resource for the A-level. That will support schools in delivering the new computing curriculum, which includes coding from key stage 1, and our reformed GCSE and A-level, both of which have a strong focus on programming."

United States of America

Internet governance

08.12.17

Reuters

[Bangladesh Bank, NY Fed discuss suing Manila bank for heist damages](#)

Bangladeshi officials have asked the Federal Reserve Bank of New York to jointly sue the Manila-based Rizal Commercial Banking Corp (RCBC) for routing stolen funds in an $81 million cyber heist back in February 2016.

"Bangladesh's central bank has asked the Federal Reserve Bank of New York to join a lawsuit it plans to file against a Philippines bank for its role in one of the world's biggest cyber-heists, several sources said."

"The Fed is yet to respond formally, but there is no indication it would join the

11.12.17

Politico

[China's ghost in Europe's telecom machine](#)

Huawei, the Chinese tech giant has been banned from bidding on Government contracts in the United States over concerns that Beijing is using the equipment for espionage. In Europe, however, Huawei is set to deliver the next generation 5G network technology.

"Huawei has succeeded in Europe where it has failed in the United States — and that's becoming a problem on the Continent."

"The Chinese tech giant is banned from bidding for government contracts in the U.S. over concerns that its telecommunication equipment could be used for spying by Beijing."

11.12.17

The Hill

[House passes Homeland Security cyber overhaul bill](#)

The House have passed legislation that will make the National Protection and Programs Directorate (NPPD) within Homeland Security its own operational agency to handle issues relating to cyber and infrastructure security.

"House lawmakers have passed legislation that would reorganize the Department of Homeland Security's cybersecurity mission."

"The House passed the legislation, which is spearheaded by Homeland Security Committee Chairman Michael McCaul (R-Texas), by a voice vote Monday evening."

12.12.17

The Hill

[Trump 'strongly' objects to cyber provision in defense bill](#)

The US President, Donald Trump has voiced his objection to a provision in the Defence Policy Bill which limits funding for the White House Communications Agency, "contingent upon the submission of a report on a national policy for cyberspace, cybersecurity, and cyberwarfare."

"President Trump is voicing strong objection to language in the defense policy bill that requires him to develop a national policy for cyberspace and cyberwarfare, charging that it and other provisions "raise constitutional concerns."

"Trump issued a statement Tuesday afternoon, just hours after he signed the fiscal 2018 National Defense Authorization Act (NDAA) into law, touting the signing as a step toward his goal of building up the U.S. military."

Cybersecurity

06.12.17

The Hill

[Army leaders launch program to recruit more cyber warriors](#)

The US Army has launched a new programme with the aim of recruiting civilians with technology and cybersecurity skills, in a drastic attempt to strengthen the US cyber force.

"The U.S. Army is officially launching a new program aimed at recruiting more cyber operators to fill existing gaps in the force."

"The service is implementing a new pilot program to directly commission civilians with technology and cybersecurity backgrounds as cyber operations officers who will provide support for the branch's Cyber Mission Force teams. "

06.12.17

The Hill

[GOP chairman warns of ISIS's 'cyber caliphate'](#)

Several lawmakers including Senator Ron Johnson have expressed their concern over the success of the Islamic State in Iraq and Syria's (ISIS) efforts to deface websites to spread and share terrorist propaganda.

"Sen. Ron Johnson (R-Wis.) joined a number of lawmakers on Wednesday raising alarm over the Islamic State in Iraq and Syria's (ISIS) success in leveraging digital platforms to recruit and spread terrorist propaganda."

"It is good that we by and large have taken away the physical caliphate," Johnson, the chair of the Senate Homeland Security and Governmental Affairs Committee, said during remarks at a hearing on evolving terror threats."

Privacy

07.12.17

The Hill

[FBI director defends bureau's hacking notification procedures amid scrutiny](#)

Christopher Wray, Director of the FBI, has explained during a congressional hearing that the FBI had followed the correct procedures in deciding not to notify US individuals that their email accounts had been hacked by Russian aligned hackers.

"FBI Director Christopher Wray on Thursday defended the bureau's procedures for notifying victims of computer hacking amid questions over U.S. individuals who were reportedly not notified of Russian efforts to breach their email accounts."

"Wray faced questions from Rep. Zoe Lofgren (D-Calif.) during a congressional hearing about a recent Associated Press report that the FBI had failed to contact dozens of U.S. targets of the Moscow-aligned hackers, who were also behind the breaches of Democrats' emails ahead of the 2016 presidential election."

10.12.17

The Hill

[**Facebook app for kids sparks privacy concerns**](#)

Facebook has designed a new chat app for children, however Democratic Senators Ed Markey and Richard Blumenthal have expressed their concern over Facebook collecting sensitive data from children.

"A new Facebook chat app designed for kids is raising concern among lawmakers and children's groups over data privacy and safety."

"The app, Messenger Kids, is targeted toward children aged 6-12, who are still too young to use Facebook. Unveiled Monday, it differs from the existing Facebook Messenger app in key ways."

Internet Inclusion

No new items of relevance

Pan-Asia

Internet governance

08.12.17

Reuters

[Bangladesh Bank, NY Fed discuss suing Manila bank for heist damages](#)

Bangladeshi officials have asked the Federal Reserve Bank of New York to jointly sue the Manila-based Rizal Commercial Banking Corp (RCBC) for routing stolen funds in an $81 million cyber heist back in February 2016.

"Bangladesh's central bank has asked the Federal Reserve Bank of New York to join a lawsuit it plans to file against a Philippines bank for its role in one of the world's biggest cyber-heists, several sources said."

"The Fed is yet to respond formally, but there is no indication it would join the suit."

11.12.17

Politico

[China's ghost in Europe's telecom machine](#)

Huawei, the Chinese tech giant has been banned from bidding on Government contracts in the United States over concerns that Beijing is using the equipment for espionage. In Europe, however, Huawei is set to deliver the next generation 5G network technology.

"Huawei has succeeded in Europe where it has failed in the United States — and that's becoming a problem on the Continent."

"The Chinese tech giant is banned from bidding for government contracts in the U.S. over concerns that its telecommunication equipment could be used for spying by Beijing."

11.12.17

Channel NewsAsia

[Singapore is already a smart nation, GovTech minister says](#)

Singapore's 'GovTech' Minister, Janil Puthucheary, believes that the nation is already a 'smart nation'. Internet development, connectivity and software in Singapore is worldclass, the minister believes, but said more needs to be done in order to understand its true ability.

"People are not necessarily aware of how smart Singapore already is, said Minister-in-charge of the Government Technology Agency (GovTech) Janil Puthucheary as he took stock of the year's progress in advancing the country's Smart Nation ambitions. Citing the example of the National Library Board (NLB), Dr. Puthucheary highlighted how users can look at and reference the entire collection of books from the comfort of their home via their mobile devices, or that one can reserve a book and pick it up from a locker after work hours."

12.12.17

Network Asia

[Only 2% of APAC companies are considered truly 'intelligent' enterprises: study](#)

According to Zebra Technologies Corporation's "Intelligent Enterprise Index" survey, only two percent of companies in the Asia Pacific region are classified as "intelligent" companies.

"Only two percent of companies in Asia Pacific are considered truly "intelligent" enterprises that leverage ties between physical and digital worlds for better visibility and actionable insights, according to Zebra Technologies Corporation's inaugural "Intelligent Enterprise Index".

"This global survey analyzes where companies are on the journey to becoming an Intelligent Enterprise; how they are connecting the physical and digital worlds to improve visibility, efficiencies and growth."

Cybersecurity

08.12.17

The Economic Times

[Chinese hackers step up attacks on Indian shores](#)

The number of cyber-attacks originating in China has increased and are likely to spread to other Asian nations such as India and Hong Kong.

"A leading Indian infrastructure company recently discovered to its dismay that its IT systems were compromised, with hackers gaining remote access to some of the most sensitive information for a fairly long period of time."

"While no official complaint has been made by the company, the attack might just be proverbial tip of the iceberg, and cyber-security experts engaged by the firm say Chinese hackers were behind the breach. Several Indian companies and some government institutions have seen an increase in cyber-attacks originating in China, say industry trackers."

10.12.17

The Hill

[German spy chief warns of Chinese cyber infiltration effort](#)

Hans-Georg Maassen, the Head of Germany's domestic intelligence agency, Bfv has warned that Chinese intelligence agencies are hacking into networks and targeting European businesses and officials. Maasen has stated that so far over 10,000 Germans have been affected.

"The head of Germany's domestic intelligence agency, BfV, said Sunday that Chinese intelligence agents are using LinkedIn to target European officials and businesses, The Associated Press reported Sunday."

"Hans-Georg Maassen said more than 10,000 Germans have been targeted by Chinese agents posing as consultants, headhunters or researchers, mainly through the professional networking site."

12.13.17

China Daily

[Cybersecurity park to fuel innovation](#)

The Chinese Government has announced its intention to create a national cybersecurity industrial park. The announcement comes as part of its plan to

enhance its big data strategy and contribute significantly to the Chinese economy.

"China aims to build a world-class national cybersecurity industrial park, which will help cultivate a 100 billion-yuan ($15 billion) cybersecurity industry in Beijing by 2020 and help the country better implement the big data strategy, officials said on Tuesday.

"The industrial park will be jointly built by Beijing municipal government and the Ministry of Industry and Information Technology. Officials expect it to help contribute more than 330 billion yuan to GDP growth by 2020. Chen Zhaoxiong, vice-minister of industry and information technology, said the booming big data industry is injecting new impetus to China's economic growth and spurring demand for safer information infrastructure."

Privacy

No new items of relevance

Internet Inclusion

10.12.17

Computer Weekly

[How Southeast Asia is keeping pace with AI](#)

Artificial Intelligence is ever increasing in Southeast Asia. Spending in AI technology is set to reach close to $5 billion, excluding Japan, by 2021.

"Forward-looking organisations in the region are embracing artificial intelligence, but uneven access to connectivity and a lack of skills and understanding of the technology are holding back wider adoption.

"Across Southeast Asia, online retailers such as Asos, Rakuten and Zalora have one thing in common – they all allow smartphone users to snap a photo of an item to perform a visual search through the use of artificial intelligence (AI) technologies"

10.12.17

Reuters

[China Telecom earmarked as Philippines' 3rd telecoms player: Manila officials](#)

China's Telecom Corp is set to become a major player in the Philippines to support the country's telecommunications infrastructure.

"State-run China Telecom Corp could become the Philippines' third telecoms player, officials of the Southeast Asian nation said on Sunday, as the government looks to stir up competition in an effort to boost notoriously poor services.

"Philippines President Rodrigo Duterte last month offered China the "privilege" of challenging a longstanding duopoly that has frustrated consumers because of slow and intermittent internet and mobile phone services."

12.12.17

NetworkAsia

[Fortinet opens doors to aspiring cybersecurity professionals at Nanyang Polytechnic](#)

Fortinet, a leading cybersecurity company has partnered with Nanyang Polytechnic in Singapore to offer cybersecurity training under the Fortinet Network Security Academy (FNSA) program.

"Nanyang Polytechnic (NYP) has become Fortinet's first partner in Singapore to jointly offer cybersecurity training under the Fortinet Network Security Academy(FNSA) program."

"The FNSA is designed to develop and train knowledgeable cybersecurity experts to manage new and advanced threats on the horizon, and NYP is the first educational institution in Singapore to offer the program. The program is also available internationally at selected organizations in Asia Pacific, the U.S., Canada, Latin America, Africa and Europe."

13.12.17

Channel NewsAsia

[Google launching artificial intelligence research Centre in China](#)

A new Artificial Intelligence Research Centre will be opened in China by Google. The aim of developing artificial intelligence has been strongly supported by the

Chinese Government but has largely restricted its use to state-owned companies.

"Alphabet Inc's Google said on Wednesday it is opening an artificial intelligence (AI) research center in China to target the country's local talent, even as the US search firm's products remain blocked in the country."

"Google said in a statement the research Centre is the first of its kind in Asia and will comprise a small team operating out of its existing office in Beijing."

Rest of the World

Internet governance

08.12.17

All Africa

[Internet Security in Africa 'Non-Existent', Experts Warn](#)

A number of cybersecurity and internet experts have stated that internet security in Africa is practically 'non-existent'.

"Data protection experts pushing for earnest legal frameworks for the privacy of Nigerians on the Internet have warned that there is no security in the African web space.

"The experts held a seminar on Tuesday in Ibadan to discuss how the worrisome situation could be addressed to avert even more debilitating realities for Internet users across the continent."

Cybersecurity

07.12.17

Reuters

[Russia calls on OSCE states to ramp up cyber security efforts](#)

Sergei Lavrov, Russia's Foreign Minister, has suggested that the Organisation for Security and Cooperation in Europe should increase its efforts on internet safety. The call from the Minister follows huge allegations by other nations of Russia cyberattacks and interference.

"Russia's foreign minister called on Organization for Security and Cooperation in Europe (OSCE) countries to strengthen efforts to ensure the safety of the internet on Thursday.

"Moscow faces widespread allegations that it interfered in the U.S. presidential election and was behind a wave of destructive global hacking attacks. It has denied any involvement in either."

08.12.17

CRN

[Australian cybersecurity spending to reach $3.8 billion in 2018: Gartner](#)

In line with its attempts to improve its cybersecurity, Australia expects to increase its spending in the area for 2018. An increase of 6.5% to nearly $4 billion is expected to be spent b to secure its digital and technological sectors.

"Australia is expected to spend $3.8 billion on cybersecurity in 2018, up 6.5 percent from 2017, according to Gartner. The research firm predicts that spending will be driven by regulations, shifting buyer mindset, awareness of emerging threats and the evolution to a digital business strategy."

"Overall, a large portion of security spending is driven by an organisation's reaction toward security breaches as more high profile cyberattacks and data breaches affect organisations worldwide," Gartner research director Ruggero Contu said."

12.12.17

The Canberra Times

[Australia ranks second in defence think tank's cyber security report](#)

Following recent efforts to increase its cybersecurity capability, Australia has successfully been ranked second for its cyber policies. The report from Australian Strategic Policy Institute revealed that only the USA performed better in this area.

"Efforts to ramp up Australia's response to the threat of attacks have placed it among the best-performing Asia-Pacific nations on a measure of their cyber capabilities."

"Defence think tank the Australian Strategic Policy Institute ranked Australia equal second with Japan out of 25 nations for cyber policies in a report released on Tuesday that said the region's nations had grown more mature in responding to the threat."

12.12.17

Front Page Africa

["Our Nation Has Potential to Leverage Cyberspace to Achieve Growth"](#)

Liberia has suggested that, with help from more advanced nations, they can achieve great advancements in the technological and cybersecurity sector. The

Foreign Minister, Marjon Kamara, believes that internet and technology will be key to the nations success in growing its economy.

"'Liberia will need help from developed countries like China, which is one of the world's major contributors and user of modern technological breakthroughs, and which has vast human capacity, in its quest and efforts to leverage cyberspace for economic development and growth,' said Foreign Minister Marjon Kamara, when she spoke at the 4th World Internet Conference 2017 in Wuzhen, China.

"Minister Kamara who led 4-man delegation to the Conference informed the audience comprising of representatives from countries around the world that, 'the Internet creates opportunities for growth and development and with the resources available to leverage these opportunities, any underdeveloped country can find its way to moving from a poor nation to a middle-income nation.'"

Privacy

07.12.17

The Hill

[FBI director defends bureau's hacking notification procedures amid scrutiny](#)

Christopher Wray, Director of the FBI, has explained during a congressional hearing that the FBI had followed the correct procedures in deciding not to notify US individuals that their email accounts had been hacked by Russian aligned hackers.

"FBI Director Christopher Wray on Thursday defended the bureau's procedures for notifying victims of computer hacking amid questions over U.S. individuals who were reportedly not notified of Russian efforts to breach their email accounts."

"Wray faced questions from Rep. Zoe Lofgren (D-Calif.) during a congressional hearing about a recent Associated Press report that the FBI had failed to contact dozens of U.S. targets of the Moscow-aligned hackers, who were also behind the breaches of Democrats' emails ahead of the 2016 presidential election."

Internet Inclusion

13.12.17

It News Africa

[Safaricom expands 4G coverage across Kenya](#)

As part of its aim of increasing internet access and connectivity, Kenya's mobile network operator, Safaricom, has revealed its intention to expand its 4G network to all 47 counties in Kenya. The news comes just three years after 4G was rolled out in the country.

"Kenya's mobile network operator, Safaricom has announced that 4G network will now be available across all 47 counties. According to the company, there are now one million customers enjoying 4G in Kenya. Safaricom said the milestone was achieved on the back of an expanding 4G network, increased the affordability of 4G smartphones and more affordable data bundles.

The country has consistently stood out as a global innovation powerhouse and a leader in global mobile technology adoption. This milestone further cements Kenya's position and establishes a strong foundation for future innovation,' said Joseph Ogutu, Director – Strategy, Safaricom"

Global Institutions

08.12.17

NATO

[**NATO and the European Union deepen cooperation on cyber defence**](#)

European Union officials have met with their counterparts at NATO's Headquarters to discuss further cooperation on cyber defence.

"*We reviewed our progress on enhancing information exchange, training and education, and exercises, while identifying new areas where more can be done – such as the sharing of best practice on crisis management and response,*" stated *Dr. Jamie Shea, NATO's Deputy Assistant Secretary General for Emerging Security Challenges.*

The officials discussed recent developments related to NATO's Cyber Defence Pledge and the implementation of NATO's decision to recognise cyberspace as a domain of operations, in addition to the new EU cybersecurity 'package'.

08.12.17

NATO

[**Joint press point**](#)

The Deputy Secretary of NATO, General Rose Gottemoeller has announced that NATO will help support cyber technology and security in the Moldovan education system by offering courses in universities.

"*Welcome—the warmest welcome possible—to the opening of the brand-new NATO Liaison Office here in Chisinau. This is a moment of great pride for the NATO Alliance, and a clear sign of the importance that we place on our relationship with Moldova.*"

"*Today is the culmination of almost 25 years of partnership between Moldova and NATO. The Liaison Office was built at the request of the Moldovan government to help drive our partnership, joining similar Liaison Offices in Kiev, Tbilisi, and Moscow.*"

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