24 January 2018

Synopsis

Scroll to read full summaries with links to news articles.

The **Indian Government** has launched a new **cybersecurity** initiative to spread awareness of **cybercrimes** and strengthen the cyber resilience of Government departments.

TRAI the Indian Telecom Regulatory Authority have recommended that **WI-FI** internet connectivity should be allowed on flights in **India**.

Australian telecommunications company **Telstra** have invested in two new Pacific submarine **cable systems** in a bid to increase connectivity between **Hongkong** and the West Coast of the **US**.

Ciaran Martin, the Chief Executive of the **National Cyber Security Centre** said it was a matter of time before the **UK** is subjected to a category-one **cyberattack** that would require a national response.

The **UK** and **France** have announced they will share expertise on sectors including **digital skills**, **cybersecurity** and **artificial intelligence**.

Finland's Nokia has won a major contract to supply **5G** wireless radio base stations to **NTT Docomo**, a Japanese telecommunications giant which provides to more than half of the **Japanese** cellular market.

The US Senate has passed **Section 702 of** the **Foreign Intelligence Surveillance Act (FISA)** by a vote of 65 to 34. This will legitimise **US surveillance** on foreigners for another six years.

The **United States** have created a **Cuba Internet Task Force** in order to examine the technological challenges and opportunities for expanding **internet access** in Cuba.

Tech company **Google** announced it would be investing in three **undersea cables** to improve its network by 2019. One of the cables will connect **California** to **Chile**.

A new **report** titled 'Internet Freedoms in Palestine: Mapping of Digital Rights Violations and Threats' discusses the decline of **internet freedoms** in **Palestinian** territories.

Palestine held a major **Digital Activism Forum** which was attended by tech giants, **Facebook** and **Google** to discuss the protection of **digital rights** and **cybercrime** law in the state.

The head of the British Army, **General Sir Nick Carter** warned that **cyberwarfare** with **Russia** now poses a bigger threat to the **United Kingdom** than terrorism.

The former **NATO** Assistant Secretary General for **Emerging Security Challenges** warned that NATO would fail to mitigate a serious **cybersecurity** attack from **Russia** due to years of "shying away" from the issue.

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

24 January 2018

Table of Contents

Europe

Internet governance

18.01.18

New Europe

Commission to table a strategy on fake news in the spring

Members of the European Parliament announced that they would table a strategy on fake news in the Spring because of Russia's success in disinformation campaigns.

"At a plenary debate in Strasbourg on January 17, Members of the European Parliament warned about Russia's propaganda influence on EU countries, calling for measures to tackle the Kremlin-orchestrated leaks, fake news, disinformation campaigns and cyber-attacks against the EU and its member states."

"Latvian MEP Sandra Kalniete from the EPP told the plenary that Europe should take the lead in setting international rules for cyberspace. "Europe drives the international agreement on climate change and it should be among the rule makers for the cyberspace," she said."

19.01.18

Euractiv

Jourova: 'Never say never' to EU hate speech law

EU justice chief Věra Jourová has threatened tech giants such as Google and Facebook with the prospect of online hate speech laws if they fail to crack down on the epidemic.

"Tech giants should share the technology they develop to detect hate speech with smaller companies, EU Justice Commissioner Vera Jourova said in an interview."

"Jourova does not want to introduce legislation requiring online platforms to take down hate speech. But she said she still won't exclude a new EU law if there is too much fragmentation as member states draft their own national rules."

22.01.18

New Europe

The United States' decision to reverse net neutrality affects the EU.

Dutch MEP Marietje Schaake urged the US Congress to restore net neutrality rules after fears the ruling will have global impactions.

"Dutch MEP Marietje Schaake, sent a letter to the US Congress on Monday urging Washington to restore net neutrality."

"The Federal Communications Commission reversed US net neutrality rules in December, meaning internet service providers in the United States will no longer treat all internet traffic equally."

22.01.18

Computer weekly

NHS England wants to use algorithms to handle NHS 111 enquiries

NHS England is seeking to use algorithms to deal with 111 enquiries online, by December 2018.

"NHS England looks at potential of processing patient enquiries using algorithms as it works on rolling out an online version of NHS 111 by December 2018."

"A leaked report has revealed NHS England is looking at the potential of handling up to 16 million NHS 111 enquiries using algorithms by 2020."

23.01.18

SC Media

UK businesses far more confident re GDPR than their European counterparts

A new study conducted by data specialist W8 Data has found that seventy percent of British business claim they understand the complexities of GDPR compared to just fifty-two and twenty-seven percent in Germany and Spain.

"More than 70 percent of British businesses are confident about their understanding of GDPR and their preparations for the upcoming data security legislation, compared to just 52 percent and 27 percent businesses in Germany and Spain respectively, new research has revealed."

"A new study conducted by data specialist W8 Data among businesses in Europe's top 10 economies has revealed the extent to which businesses

understand the rules laid out in the GDPR and their level of preparedness for the new law which will come into effect on 25 May."

Cybersecurity

18.01.18

SC Media

Cyber-attacks one of the biggest threats to the world in 2018 says WEF

According to the World Economic Forum's Global Risks Report, cyber-attacks pose one of the biggest threats to the world.

"Cyber-crime joins environmental disasters, large-scale involuntary migration and illicit trade as one of the most notable risks in the world this year, according to the latest Global Risks Report just brought out by WEF."

"The main issue globally, as with previous years, still remains as weapons of mass destruction, according to CNBC, which reported on the WEF Global Risks Report, however, now the next three most notable risks are environmental concerns because of how much damage they cause to land and property."

22.01.18

Computer Weekly

UK urged to up spending on cyber defence

UK defence Chief of General Staff Nick Carter urged the UK Government to spend more on cyber defence to mitigate threats from foreign countries.

"Cyber-attacks that target military and civilian operations are one of the biggest threats facing the UK, according to a top military officer, but security experts say cyber defence spending must be carefully considered."

"The UK needs to keep up with its adversaries, such as Russia, to avoid being exposed to unorthodox, hybrid warfare that combines traditional conflict with cyber warfare, UK defence chief of general staff Nick Carteris expected to warn."

23.01.18

Independent

[Cyberwarfare with Russia 'now greater threat than terrorism', warns British Army chief]

The head of the British Army, General Sir Nick Carter warned that cyberwarfare with Russia now poses a bigger threat to the United Kingdom than terrorism.

"Enemy states using hybrid "weapons" ranging from assassinations and cyber-attacks to the use of fake news and corruption now pose a greater threat to the UK and the West than terrorism, the head of the British Army has warned."

"Vladimir Putin's Russia is the "arch exponent" of this form of clandestine combat and "represents the most complex and capable state-based threat to our country since the end of the Cold War", said General Sir Nick Carter, adding that this was also the view of fellow commanders in the US, France and Germany."

23.01.18

Public Technology

[Major cyberattack on UK likely in next two years, warns NCSC chief]

Ciaran Martin, the Chief Executive of the National Cyber Security Centre said it was a matter of time before the UK is subjected to a category-one cyberattack that would require a national response.

"The chief executive of the National Cyber Security Centre Ciaran Martin has warned that a category-one cyberattack on the UK is an inevitability."

"Martin added that the country will probably suffer such an attack at some point in the next two years. A category-one attack would require a national response, and could include an attempt to harm an election process, or an assault that brought down energy infrastructure or banking services. An aggressive cyber incursion from a rogue nation could also be classed in category one. Last year's WannaCry ransomware attack that impacted the NHS was considered as a category-two attack."

Privacy

23.01.18

Reuters

Facebook to hand privacy controls to users ahead of EU law

Facebook's Chief Operating Officer Sheryl Sandberg said users of the social media networking site will be given more control of their data, ahead of the new EU data protection rules.

"Facebook will make it easier for its more than 2 billion users to manage their own data in response to a tough new European Union law that comes into force in May, the social network's Chief Operating Officer Sheryl Sandberg said."

"We're rolling out a new privacy centre globally that will put the core privacy settings for Facebook in one place and make it much easier for people to manage their data," Sandberg said at a Facebook event in Brussels on Tuesday."

Internet Inclusion

18.01.18

Computer Weekly

Tech has 'disconnect' between the skills students are taught and the abilities firms need

According to experts at Change Catalyst's London Tech Inclusion event the technology industry is not communicating with educational providers about the skills graduates need for the workplace, leaving several unemployed.

"Many tech graduates face unemployment because their skills do not meet employers' requirements, say experts at Change Catalyst's London Tech Inclusion event."

"There is a "disconnect" between the technology industry and education providers, according to a panel of experts."

19.01.18

Computer Weekly

UK and France to collaborate on digital tech

The UK and France have announced they will share expertise on sectors including digital skills, cybersecurity and artificial intelligence.

"The UK and French governments have joined forces to increase technology and innovation cooperation between the two nations."

"The UK and France have teamed up to seize the economic and social benefits of new technologies such as artificial intelligence (AI) and automation. The joint strategy includes plans for a future digital conference, where experts from both countries will come together and share knowledge and skills on a range of issues such as AI, cyber security and digital skills."

19.01.18

Reuters

Nokia signs its first official 5G equipment deal with NTT DoCoMo

Finland's Nokia has won a major contract to supply 5G wireless radio base stations to NTT Docomo, a Japanese telecommunications giant which provides to more than half of the Japanese cellular market.

"Finland's Nokia said on Friday it signed its first major deal to supply new 5G wireless radio base stations to Japanese telecom operator NTT DoCoMo, which boasts nearly half of the country's mobile subscribers."

"The contract marks Nokia's first sizeable deal for its flagship mobile base station equipment based on official global New Radio (NR) standards for the fifth generation of wireless networks, which were only finalised in December 2017."

United States of America

Internet governance

17.01.18

SC Media

US DETER Act aimed at punishing Russia and other nation-states

The US Defending Elections from Threats by Establishing Redlines Act (DETER) seeks to reprimand foreign actors such as Russia, North Korea and China if they interfere in US elections.

"In the US, a bipartisan bill that takes aim at protecting the US elections from nation-state attacks would compel the Trump administration to levy harsh punishment on Russia for further interfering in US elections."

"In the US, a bipartisan bill that takes aim at protecting the US elections from nation-state attacks would compel the Trump administration to levy harsh punishment on Russia for further interfering in US elections and outlines the actions that would prompt the government to retaliate against other countries like China and North Korea if they similarly meddle."

18.01.18

SC Media

Senate passes FISA Amendments Reauthorization Act

The US Senate has passed Section 702 of the Foreign Intelligence Surveillance Act (FISA) by a vote of 65 to 34. This will re-legitimise US surveillance on foreigners for another six years.

"A six-year extension to the much-debated Section 702 of the Foreign Intelligence Surveillance Act (FISA) will soon be on its way to the White House for the president to sign after the Senate gave it a nod by a vote of 65 to 34."

"The House passed the bill on Jan. 11, even after a pair of contradictory tweets from President Trump over his take on the proposed legislation momentarily threw lawmakers into confusion over his position."

22.01.18

New Europe

The United States' decision to reverse net neutrality affects the EU.

Dutch MEP Marietje Schaake urged the US Congress to restore net neutrality rules after fears the ruling will have global impactions.

"Dutch MEP Marietje Schaake, sent a letter to the US Congress on Monday urging Washington to restore net neutrality."

"The Federal Communications Commission reversed US net neutrality rules in December, meaning internet service providers in the United States will no longer treat all internet traffic equally."

Cybersecurity

17.01.18

NextGov

As America's Nukes and Sensors Get More Connected, the Risk of Cyber Attack Is Growing

The United States are shoring up their nuclear weapons arsenal, however, the more connected these systems are to digital technology the more vulnerable they are to cyber-attacks.

"Future nuclear weapons will be more sophisticated and better integrated with other equipment. That has benefits and drawbacks."

"Building nuclear weapons and warning systems that can be relied upon is harder than it was during the Cold War, thanks to the growing number of digital connections between various parts of the nuclear enterprise."

18.01.18

SC Media

Cyber-attacks one of the biggest threats to the world in 2018 says WEF

According to the World Economic Forum's Global Risks Report, cyber-attacks pose one of the biggest threats to the world.

"Cyber-crime joins environmental disasters, large-scale involuntary migration and illicit trade as one of the most notable risks in the world this year, according to the latest Global Risks Report just brought out by WEF."

"The main issue globally, as with previous years, still remains as weapons of mass destruction, according to CNBC, which reported on the WEF Global Risks Report, however, now the next three most notable risks are environmental concerns because of how much damage they cause to land and property."

23.01.18

Computer Weekly

Facebook offers funding to secure the internet

Facebook said if researchers at universities, non-profit organisations or non-governmental organisations find ways to improve security online, they will award them with $100,000.

"Facebook is offering grants of up to $100,000 to researchers at universities, non-profit organisations and non-governmental organisations to improve security online."

"The social networking firm announced its Secure the Internet Grants initiative as part of its commitment to fund security research."

Privacy

17.01.18

Reuters

Twitter may notify users exposed to Russian propaganda during 2016 election

Tech giant Twitter is contemplating whether to notify the victims of Russian propaganda in the run up to the 2016 general election.

"Twitter may notify users whether they were exposed to content generated by a suspected Russian propaganda service, a company executive told U.S. lawmakers on Wednesday."

"The social media company is "working to identify and inform individually" its users who saw tweets during the 2016 U.S. presidential election produced by accounts tied to the Kremlin-linked Internet Research Army, Carlos Monje, Twitter's director of public policy, told the U.S. Senate Commerce, Science and Transportation Committee."

23.01.18

Reuters

Facebook to hand privacy controls to users ahead of EU law

Facebook's Chief Operating Officer Sheryl Sandberg said users of the social media networking site will be given more control of their data, ahead of the new EU data protection rules.

"Facebook will make it easier for its more than 2 billion users to manage their own data in response to a tough new European Union law that comes into force in May, the social network's Chief Operating Officer Sheryl Sandberg said."

"We're rolling out a new privacy centre globally that will put the core privacy settings for Facebook in one place and make it much easier for people to manage their data," Sandberg said at a Facebook event in Brussels on Tuesday."

Internet Inclusion

17.01.18

Financial Times

Google quietly opens third China office

US tech company, Google has opened another office in China even though many of its services are blocked in the country.

"Google has quietly opened a third office in China, highlighting its growing hardware and ad business in the country even as the US Tech company's signature search engine remains blocked there."

"The new office is in Shenzhen, the former fishing village turned Asian Silicon Valley that borders Hong Kong and is home to Chinese tech giants including Tencent and Huawei."

17.01.18

Nextgov

Google To Build 3 Undersea Internet Cables

Tech company Google announced it would be investing in three undersea cables to improve its network by 2019. One of the cables will connect California to Chile.

"The tech company announced it has made plans for three undersea cables to improve its network. The cables will be commission in 2019."

"The areas connected by the cables will have access to a faster and better version of Google's products, such as their cloud platform and G Suite services, according to Google."

22.01.18

Computer Weekly

Telstra invests in two new submarine cables to bolster Asia-US connectivity

Australian telecommunications company Telstra have invested in two new Pacific submarine cable systems in a bid to increase connectivity between Hongkong and the West Coast of the US.

"The Hong Kong Americas and Pacific Light Cable Network cables will provide more robust connectivity to support the Asia-Pacific region's growing internet traffic."

"Australian telco Telstra is investing in two subsea cables that will connect Hong Kong and the US west coast, shoring up connectivity between Asia and the US."

22.01.18

Gadgets Now

WhatsApp for Business to start rolling out in India this week

Instant-messaging app, WhatsApp is rolling out WhatsApp for business in India and Brazil this week.

"The world's most-widely used instant-messaging app WhatsApp rolled out its WhatsApp for Business app in select countries late last week. Though the company did say that the app will soon roll out in India and Brazil, two of its biggest market, it didn't reveal a specific timeframe for the same."

"The company said that the app will be coming to these countries in the next few weeks, the company said in its blog post."

24.01.18

Computer Weekly

AWS opens third availability zone in Singapore

Cloud major Amazon Web Services (AWS) announced the opening of a third 'availability zone' in Singapore in a bid to support the rapid expansion of the AWS customer base in the Asia-Pacific region.

"Cloud service provider is upping the ante in a region that has been lapping up cloud infrastructure services to advance digitisation efforts."

"Amazon Web Services (AWS) has opened a third availability zone in Singapore, underscoring the growing appetite for cloud infrastructure services in Southeast Asia."

24.01.18

Channel NewsAsia

US State Department creates Cuba Internet Task Force

The United States have created a Cuba Internet Task Force in order to examine the technological challenges and opportunities for expanding internet access in Cuba.

"The U.S. State Department said on Tuesday that it had created a Cuba Internet Task Force to promote "the free and unregulated flow of information" on the Communist-run island, an action denounced by Cuban state media as subversive."

"The task force will examine the technological challenges and opportunities for expanding internet access and independent media in Cuba," the agency said in a statement. It said the task force of U.S. government and non-governmental representatives would meet for the first time on Feb. 7."

Pan-Asia

Internet governance

17.01.18

SC Media

US DETER Act aimed at punishing Russia and other nation-states

The US Defending Elections from Threats by Establishing Redlines Act (DETER) seeks to reprimand foreign actors such as Russia, North Korea and China if they interfere in US elections.

"In the US, a bipartisan bill that takes aim at protecting the US elections from nation-state attacks would compel the Trump administration to levy harsh punishment on Russia for further interfering in US elections."

"In the US, a bipartisan bill that takes aim at protecting the US elections from nation-state attacks would compel the Trump administration to levy harsh punishment on Russia for further interfering in US elections and outlines the actions that would prompt the government to retaliate against other countries like China and North Korea if they similarly meddle."

22.01.18

China Daily

China calls for deeper cooperation on internet of things

He Xuming, Executive Chairman of the World Internet of Things Convention Forum in China urged countries across the world to increase collaboration on internet of things.

"China is calling for deeper cooperation on the internet of things among countries around the world, and to jointly launch a global demonstration platform for the IoT, said He Xuming, executive chairman of the World Internet of Things Convention."

"The formation of the World IoT platform will bring tens of millions of dollars to the global economic markets," He said during the World IoT Innovation and Application Forum in Beijing on Monday."

Cybersecurity

18.01.18

SC Media

Cyber-attacks one of the biggest threats to the world in 2018 says WEF

According to the World Economic Forum's Global Risks Report, cyber-attacks pose one of the biggest threats to the world.

"Cyber-crime joins environmental disasters, large-scale involuntary migration and illicit trade as one of the most notable risks in the world this year, according to the latest Global Risks Report just brought out by WEF."

"The main issue globally, as with previous years, still remains as weapons of mass destruction, according to CNBC, which reported on the WEF Global Risks Report, however, now the next three most notable risks are environmental concerns because of how much damage they cause to land and property."

19.01.18

Security Brief Asia

HKPC to Hong Kong businesses: Be prepared for financially-motivated cyber-attacks in 2018

The Hong Kong Productivity Council has warned businesses in the territory that cyber-attacks will become more financially motivated in 2018 and urged them to become more cyber resilient.

"The Hong Kong Productivity Council (HKPC) says that cybercrimes against Hong Kong businesses are more likely to be financially-motivated this year and warns that everyone should strengthen their defences against ransom-based attacks."

"According to the Hong Kong Computer Emergency Response Team (HKCERT), there were 6506 security incidents reported last year - a 7% increase since 2017."

19.01.18

The Economic Times

Govt launches Cyber Surakshit Bharat initiative in partnership with top tech companies

The Indian Government has launched a new Cybersecurity initiative to spread awareness of cybercrimes and strengthen the cyber resilience of Government departments.

"In order to strengthen cyber security practices and awareness among the government departments, the ministry of electronics and IT has launched the Cyber Surakshit Bharat initiative in association with the IT industry majors."

"An aim of the initiative is to spread awareness about cybercrime and building capacity for safety measures for Chief Information Security Officers (CISOs) and frontline IT staff across all government departments."

Privacy

No new items of relevance

Internet Inclusion

17.01.18

Financial Times

Google quietly opens third China office

US tech company, Google has opened another office in China even though many of its services are blocked in the country.

"Google has quietly opened a third office in China, highlighting its growing hardware and ad business in the country even as the US Tech company's signature search engine remains blocked there."

"The new office is in Shenzhen, the former fishing village turned Asian Silicon Valley that borders Hong Kong and is home to Chinese tech giants including Tencent and Huawei."

19.01.18

Channel NewsAsia

TRAI recommends allowing in-flight internet connectivity

TRAI the Indian Telecom Regulatory Authority have recommended that WI-FI internet connectivity should be allowed on flights in India.

"The Telecom Regulatory Authority of India (TRAI) on Friday recommended that internet services like wi-fi and mobile connectivity should be permitted on domestic and international flights in India."

"India is one of the world's fastest-growing aviation markets and also the world's fastest growing internet services market, and such a step is likely to boost revenue for service providers as well as airlines."

22.01.18

Computer Weekly

Telstra invests in two new submarine cables to bolster Asia-US connectivity

Australian telecommunications company Telstra have invested in two new Pacific submarine cable systems in a bid to increase connectivity between Hongkong and the West Coast of the US.

"The Hong Kong Americas and Pacific Light Cable Network cables will provide more robust connectivity to support the Asia-Pacific region's growing internet traffic."

"Australian telco Telstra is investing in two subsea cables that will connect Hong Kong and the US west coast, shoring up connectivity between Asia and the US."

22.01.18

Gadgets Now

WhatsApp for Business to start rolling out in India this week

Instant-messaging app, WhatsApp is rolling out WhatsApp for business in India and Brazil this week.

"The world's most-widely used instant-messaging app WhatsApp rolled out its WhatsApp for Business app in select countries late last week. Though the

company did say that the app will soon roll out in India and Brazil, two of its biggest market, it didn't reveal a specific timeframe for the same."

"The company said that the app will be coming to these countries in the next few weeks, the company said in its blog post."

24.01.18

Computer Weekly

AWS opens third availability zone in Singapore

Cloud major Amazon Web Services (AWS) announced the opening of a third 'availability zone' in Singapore in a bid to support the rapid expansion of the AWS customer base in Asia-Pacific region.

"Cloud service provider is upping the ante in a region that has been lapping up cloud infrastructure services to advance digitisation efforts."

"Amazon Web Services (AWS) has opened a third availability zone in Singapore, underscoring the growing appetite for cloud infrastructure services in Southeast Asia."

Rest of the World

Internet governance

17.01.18

SC Media

US DETER Act aimed at punishing Russia and other nation-states

The US Defending Elections from Threats by Establishing Redlines Act (DETER) seeks to reprimand foreign actors such as Russia, North Korea and China if they interfere in US elections.

"In the US, a bipartisan bill that takes aim at protecting the US elections from nation-state attacks would compel the Trump administration to levy harsh punishment on Russia for further interfering in US elections."

"In the US, a bipartisan bill that takes aim at protecting the US elections from nation-state attacks would compel the Trump administration to levy harsh punishment on Russia for further interfering in US elections and outlines the actions that would prompt the government to retaliate against other countries like China and North Korea if they similarly meddle."

18.01.18

New Europe

Commission to table a strategy on fake news in the spring

Members of the European Parliament announced that they would table a strategy on fake news in Spring because of Russia's success in disinformation campaigns.

"At a plenary debate in Strasbourg on January 17, Members of the European Parliament warned about Russia's propaganda influence on EU countries, calling for measures to tackle the Kremlin-orchestrated leaks, fake news, disinformation campaigns and cyber-attacks against the EU and its member states."

"Latvian MEP Sandra Kalniete from the EPP told the plenary that Europe should take the lead in setting international rules for cyberspace. "Europe drives the international agreement on climate change and it should be among the rule makers for the cyberspace," she said."

Cybersecurity

18.01.18

SC Media

Cyber-attacks one of the biggest threats to the world in 2018 says WEF

According to the World Economic Forum's Global Risks Report, cyber-attacks pose one of the biggest threats to the world.

"Cyber-crime joins environmental disasters, large-scale involuntary migration and illicit trade as one of the most notable risks in the world this year, according to the latest Global Risks Report just brought out by WEF."

"The main issue globally, as with previous years, still remains as weapons of mass destruction, according to CNBC, which reported on the WEF Global Risks Report, however, now the next three most notable risks are environmental concerns because of how much damage they cause to land and property."

16.01.18

The Express

NATO alliance is NOT READY to defend against cyber warfare with Russia, top expert warns

The former NATO Assistant Secretary General for Emerging Security Challenges warned that NATO would fail to mitigate a serious cybersecurity attack from Russia due to years of "shying away" from the issue.

"NATO is not ready to defend against a major cyber-attack from its adversaries after years of "shying away" from the threat, one of the top experts in the field has warned."

"The western alliance has been in a "state of denial" about the danger posed by hackers acting on behalf of countries such as Russia and China, Ambassador Sorin Ducaru said."

23.01.18

Independent

Cyberwarfare with Russia 'now greater threat than terrorism', warns British Army chief

The head of the British Army, General Sir Nick Carter warned that cyberwarfare with Russia now poses a bigger threat to the United Kingdom than terrorism.

"Enemy states using hybrid "weapons" ranging from assassinations and cyber-attacks to the use of fake news and corruption now pose a greater threat to the UK and the West than terrorism, the head of the British Army has warned."

"Vladimir Putin's Russia is the "arch exponent" of this form of clandestine combat and "represents the most complex and capable state-based threat to our country since the end of the Cold War", said General Sir Nick Carter, adding that this was also the view of fellow commanders in the US, France and Germany."

Privacy

17.01.18

Reuters

Twitter may notify users exposed to Russian propaganda during 2016 election

Tech giant Twitter is contemplating whether to notify the victims of Russian propaganda in the run up to the 2016 general election.

"Twitter may notify users whether they were exposed to content generated by a suspected Russian propaganda service, a company executive told U.S. lawmakers on Wednesday."

"The social media company is "working to identify and inform individually" its users who saw tweets during the 2016 U.S. presidential election produced by accounts tied to the Kremlin-linked Internet Research Army, Carlos Monje, Twitter's director of public policy, told the U.S. Senate Commerce, Science and Transportation Committee."

Internet Inclusion

18.01.18

APC

Major international digital activism forum takes place in Palestine

Palestine held a major Digital Activism Forum which was attended by tech giants, Facebook and Google to discuss the protection of digital rights and cybercrime law in the state.

"What are the global trends in digital activism? How can digital rights be protected in Palestine and globally? How can Palestinian innovation in digital activism be promoted? These were some of the issues addressed during

the second Palestine Digital Activism Forum that was held in Ramallah on 17 January 2018."

"Hundreds of students, activists and human rights defenders attended the Forum, hosted by 7amleh – the Arab Center for Social Media Advancement, a non-profit organisations aimed at enabling Palestinian and Arab civil society to effectively utilise the tools of digital advocacy."

22.01.18

Computer Weekly

Telstra invests in two new submarine cables to bolster Asia-US connectivity

Australian telecommunications company Telstra have invested in two new Pacific submarine cable systems in a bid to increase connectivity between Hongkong and the West Coast of the US.

"The Hong Kong Americas and Pacific Light Cable Network cables will provide more robust connectivity to support the Asia-Pacific region's growing internet traffic."

"Australian telco Telstra is investing in two subsea cables that will connect Hong Kong and the US west coast, shoring up connectivity between Asia and the US."

23.01.18

APC

7amleh publishes innovative research on internet freedoms in Palestine

A new report titled 'Internet Freedoms in Palestine: Mapping of Digital Rights Violations and Threats' discusses the decline of internet freedoms such as privacy online and the freedom of expression in Palestinian territories.

"The new report titled "Internet freedoms in Palestine: Mapping of digital rights violations and threats", available in English and Arabic, constitutes the first of its kind on the Palestinian level."

Global Institutions

16.01.18

The Express

NATO alliance is NOT READY to defend against cyber warfare with Russia, top expert warns

The former NATO Assistant Secretary General for Emerging Security Challenges warned that NATO would fail to mitigate a serious cybersecurity attack from Russia due to years of "shying away" from the issue.

"NATO is not ready to defend against a major cyber-attack from its adversaries after years of "shying away" from the threat, one of the top experts in the field has warned."

"The western alliance has been in a "state of denial" about the danger posed by hackers acting on behalf of countries such as Russia and China, Ambassador Sorin Ducaru said."

18.01.18

SC Media

Cyber-attacks one of the biggest threats to the world in 2018 says WEF

According to the World Economic Forum's Global Risks Report, cyber-attacks pose one of the biggest threats to the world.

"Cyber-crime joins environmental disasters, large-scale involuntary migration and illicit trade as one of the most notable risks in the world this year, according to the latest Global Risks Report just brought out by WEF."

"The main issue globally, as with previous years, still remains as weapons of mass destruction, according to CNBC, which reported on the WEF Global Risks Report, however, now the next three most notable risks are environmental concerns because of how much damage they cause to land and property."

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

Cyber Security and Data Opportunities in Sub-Saharan Africa – 05.03.18

London, England

Living in the Internet of Things- Cybersecurity of the IoT – 28.03.18-29.03.18

London, England

RSA – 16.04.18–20.04.18

San Francisco, USA

Data Centre Risk Radar- Technical Skills Shortage – 26.04.18

London, England

Africa Internet Summit – 29.04.18-11.05.18

Dakar, Senegal