25 July 2018

Synopsis

Scroll to read full summaries with links to news articles.

According to **Le Thi Thu Hang**, a spokesperson for the **Foreign Ministry of Vietnam** said the country's new **cybersecurity** law will create a 'safe and healthy cyberspace' and protect rights online. However, critics argue it grants the Government more power to 'crackdown on dissent.'

The **Singaporean Government** have announced that the biggest ever **cyber-attack** has seen the personal information of 1.5 million people stolen and the Prime Minister **Lee Hsien Loong** was also targeted. The data stolen includes names, NRIC numbers, addressees, gender, race and date of birth.

Cuba has announced plans to allow the **internet** to be rolled out on **mobile phones** by the end of the year. This is part of a wider strategy to get more people connected to the internet and boost the economy.

At **G20** meeting, European finance leaders and bankers urged for global rules to tax the **digital economy** to ensure technology giants such as **Google**, **Facebook** and **Amazon** pay more **tax**.

Seventeen **UK** organisations in the **cybersecurity** industry including the **Chartered Institute for IT**, **Chartered Institute of Personnel and Development** and **techUK** have collaborated to create a national professional body for cybersecurity. Their aim is to address the skills gap.

New concerns over user **data sharing** has led internet giant **Facebook** to suspend analytics firm **Crimson Hexagon**, a company which offers consumer insights and has contracts with Government agencies across the world including **Russia** and **Turkey**. According to the **Wall Street Journal**, Crimson Hexagon has "contracts to analyse public Facebook data for clients including a Russian non-profit with ties to the Kremlin and multiple US government agencies."

Internet giant **Google** is facing a $5 billion **fine** from the **European Commission** over its **Android** mobile operating system. CEO of Google **Sundar Pichai** said "we'll appeal the Commission's decision and take the due process available to us."

A new Bill which applies only to **Homeland Security** contracts would grant the Department with powers to ban technology contractors that they deemed a **cybersecurity** risk. In some cases, they won't have to notify contractors and contractors won't be able to challenge the decision in a federal court or through the Government Accountability Office's.

NATO have agreed to create two new bodies, a **cyberspace operations center** in Belgium and a '**Joint Force Command'** in Norfolk, Virginia, to deal with the **cybersecurity** threat and spread of 'disinformation campaigns.'

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

25 July 2018

Table of Contents

Europe

Internet governance

23.07.18

Euractiv

Europeans press for digital tax at G20 meeting

At G20 meeting, European finance leaders and bankers urged for global rules to tax the digital economy to ensure technology giants such as Google, Facebook and Amazon pay more tax.

"European finance leaders called for progress on global rules to tax the digital economy at a meeting of G20 finance ministers and central bankers in Argentina on Sunday (22 July), putting them at odds with US counterparts."

"The final communique reaffirmed a commitment to address the impacts of the shift to a digital economy on the international tax system by 2020, without giving more details."

Cybersecurity

12.07.18

Fifth Domain

NATO summit boosts cybersecurity amid uncertainty

NATO have agreed to create two new bodies, a cyberspace operations center in Belgium and a 'Joint Force Command' in Norfolk, Virginia, to deal with the cybersecurity threat and spread of 'disinformation campaigns.'

"Amid uncertainty over NATO member's defense spending, energy deals with Russia and the very future of the alliance itself, combating Moscow's campaign of digital war quietly emerged as an item of agreement for the 29-state body during a summit in Brussels."

"Consider: Few previous NATO meetings of world leaders have included so much discussion over cybersecurity. In a joint declaration, the word "cyber" appeared 26 times. In what appears to be a first for the alliance, leaders twice mentioned the threat of "disinformation campaigns," that have spread chaos through western countries. The declaration devoted two sections to digital security."

17.07.18

CNN

Russia plans to increase aggression post-World Cup

CNN has reported that Russian intelligence agencies are planning to increase operations targeting Western countries now that the World Cup and the Trump Putin Helsinki summit has ended.

"Russian intelligence agencies are planning to ramp up operations targeting western countries now that the World Cup and the Trump-Putin Helsinki summit have ended, according to sources familiar with intelligence collected by the United Kingdom, the US and other allies."

"The concern about Russia's intentions preceded this week's meeting between President Donald Trump and Russian President Vladimir Putin."

19.07.18

SC Media

National professional body for cyber sec established - combines 17 orgs - just as gov criticised for inaction

Seventeen UK organisations in the cybersecurity industry including the Chartered Institute for IT, Chartered Institute of Personnel and Development and techUK have collaborated to create a national professional body for cybersecurity. Their aim is to address the skills gap.

"A grand Alliance of 17 leading UK organisations impacting cyber-security has been formed in response to a call by the UK government's Department of Digital, Culture, Media and Sport (DCMS) to develop a national professional body for cyber-security."

"The DCMS has only just begun a consultation process - open until 5 pm 31 August, inviting those interested to contribute to how the country can improve the environment to develop people with the right skills, capabilities and professionalism to meet its need for cyber-security professionals."

Privacy

17.07.18

Euractiv

EU to slam Google with record fine ahead of Juncker US visit

Internet giant Google is facing a $5 billion fine from the European Commission over its Android mobile operating system. CEO of Google Sundar Pichai said "we'll appeal the Commission's decision and take the due process available to us."

"Google is set to face a record-busting EU antitrust fine this week over its Android mobile operating system but rivals hoping that an order to halt unfair business practices will help them may be disappointed."

"The European Commission's decision, delayed by a week by US President Donald Trump's visit to a NATO summit in Brussels last week, is expected on Wednesday."

Internet Inclusion

12.07.18

Computer Weekly

Half of young girls don't think tech careers are exciting

According to research by fashion e-commerce group YOOX Net-a-Porter (YNAP), half of young women are aware of technology related careers however they do not pursue them because they perceive such careers as "unexciting."

"Young women are put off of technology careers because they don't perceive them to be exciting, according to research."

"Half of young women know about technology careers but think they are "unexciting", according to research by fashion e-commerce group YOOX Net-a-Porter (YNAP)."

12.07.18

Financial Times

MBA courses start offering digital security skills

From September, Coventry University will offer cyber security MBA courses to students, with regular MBA students being offered additional modules within the specialism.

"When Coventry University ran its MBA students through a simulated cyber-attack, few of them knew what to do, and most expected IT professionals to take the lead."

"You put a team in a room and tell them, 'You've been attacked, what do you do?' and usually everyone turns to the techie guy." Says Anitha Chinnaswamy, course director for Coventry's Cyber Security Management MBA."

16.07.18

UK Parliament

Cyber Security Skills and the UK's Critical National Infrastructure

The Joint Committee on the National Security Strategy has published a report into Cyber Security Skills and the UK's Critical National Infrastructure, as part of its broader inquiry and evidence sessions into cyber security and CNI. The report stipulated that the UK's critical national infrastructure sector is being negatively impacted by the lack of cyber security skills and described this issue as a "pressing matter of national security."

"Cyber security is not just about technology. It is about people, and the range of technical and specialist skills that are needed to ensure that the services, systems and networks we use every day are secure."

"During our ongoing inquiry into the cyber security of the UK's critical national infrastructure (CNI), we heard that although the UK has one of the most vibrant digital economies in the world, there is not currently the cyber security skills base to match, with both the Government and private sector affected by the shortage in skills."

17.07.18

Computer Weekly

Code First: Girls teaches more women to code in UK than universities

Code First, a Not for Profit Social Enterprise have partnered with BT, a British multinational telecommunications company to offer more women the opportunity to learn tech skills. According to Computer Weekly, by 2018 'Code First: Girls will be teaching an average of around 5,000 women to code each year, which is more than the annual number of women studying coding-based subjects across the UK's university system.'

"Social enterprise partners with BT to offer more women the opportunity to learn tech skills."

"By the end of 2018, Code First: Girls will be teaching an average of 5,000-5,500 women to code each year, which is more than the annual number of women studying coding-based subjects across the UK's university system."

18.07.18

Computer Weekly

Deloitte launches EMEA-wide initiative to close cyber security gender gap

Deloitte, a UK-incorporated multinational professional services network has launched a Women in Cyber initiative to help close the gender gap in the cybersecurity sector. Their aim is to create more awareness of the gender gap and help facilitate an environment which encourages women to pursue a career in cybersecurity.

"Professional services organisation Deloitte expands its UK efforts to encourage more women into cyber security to cover the EMEA area."

"Deloitte has launched an EMEA Women in Cyber initiative in an attempt to help close the gender gap in the cyber security sector."

18.07.18

Computer Weekly

Cyber security top priority for aircraft makers, says Airbus

According to an interview with Ian Goslin, UK Managing Director for Cyber Security at Airbus, everything the air manufacturing industry plans is "considered through the lens of cyber security."

"There is a high level of collaboration in the aircraft industry on cyber security, but not all other industries are at the same level, according to an industry veteran at multinational aerospace and defence firm Airbus."

"Everything the air manufacturing industry plans is considered through the lens of cyber security, but not everyone is up to the same standard across the industry in general, even among suppliers of critical national infrastructure, said Ian Goslin, UK managing director of Airbus cyber security."

19.07.18

Department for Digital, Culture Media and Sport

Implementing the national cybersecurity strategy- developing the cybersecurity profession in the UK

The Department for Digital, Culture, Media and Sport (DCMS) released a new consultation on Implementing the Cyber Security Strategy: Developing the Cyber Security Profession in the UK. The consultation sets out proposals based around four key areas to develop the skills, capacities and professionalism of the cyber security industry, which was a key area of activity in the National Cyber Security Strategy.

"The UK has some of the best cyber security professionals in the world. They play a critical and ever-increasing role in not only the UK's national security, but also in realising the government's ambition to make the UK the safest place in the world to be online and the best place in the world to start and grow a digital business."

"Since the National Cyber Security Strategy was published in 2016, the cyber threat has continued to diversify and grow, bringing in to even sharper focus the need to develop our capability."

20.07.18

The Sun

Firm uses brain-teaser games to find hidden cyber-security talents in Forces veterans

Cybersecurity experts at Immersive labs, a cybersecurity startup that helps companies identify and develop talent has created a new software which gives veterans the opportunity to play online games to help them break into cyber jobs.

"VETERANS are being urged to tackle ingenious online challenges in a bid to find "hidden" cyber sleuths – echoing the brain teasers used to spot WWII code breakers."

“Tech boffins at cyber company Immersive Labs – backed by a former Director of spy station GCHQ – has developed software to help forces leavers break into cyber jobs.”

United States of America

Internet governance

24.07.18

Nextgov

NDAA Conference: Congress Spares DISA, Bans Chinese Firms and Orders JEDI Review

The National Defense Authorisation Act has a provision within it that bans technology provided by the Chinese telecommunication firms Huawei and ZTE and from cybersecurity firm Kaspersky.

"The Defense Information Systems Agency came out a winner in the conference version of the National Defense Authorization Act, an annual must-pass defense policy bill released Monday."

"First, Senate conferees watered down a House provision that would have transferred DISA's responsibility for day-to-day defense of Defense Department information networks to U.S. Cyber Command."

24.07.18

Next Gov

Homeland Security Committee Forwards Bill to Prevent the Next Kaspersky

A new Bill which applies only to Homeland Security contracts would grant the Department with powers to ban technology contractors that they deemed a cybersecurity risk. In some cases, they won't have to notify contractors and contractors won't be able to challenge the decision in a federal court or through the Government Accountability Office's.

"The Homeland Security Department would have broad authority to bar technology contractors that officials believe pose cybersecurity and national security risks under legislation forwarded by the House Homeland Security Committee Tuesday."

"The bill, which would only apply to Homeland Security contracts, would generally require the department to notify contractors before a ban and allow them to protest the ban or make efforts to mitigate the problem."

Cybersecurity

12.07.18

Fifth Domain

NATO summit boosts cybersecurity amid uncertainty

NATO have agreed to create two new bodies, a cyberspace operations center in Belgium and a 'Joint Force Command' in Norfolk, Virginia, to deal with the cybersecurity threat and spread of 'disinformation campaigns.'

"Amid uncertainty over NATO member's defense spending, energy deals with Russia and the very future of the alliance itself, combating Moscow's campaign of digital war quietly emerged as an item of agreement for the 29-state body during a summit in Brussels."

"Consider: Few previous NATO meetings of world leaders have included so much discussion over cybersecurity. In a joint declaration, the word "cyber" appeared 26 times. In what appears to be a first for the alliance, leaders twice mentioned the threat of "disinformation campaigns," that have spread chaos through western countries. The declaration devoted two sections to digital security."

14.07.18

Channel NewsAsia

US intel chief warns of devastating cyber threat to US infrastructure

Dan Coats, Director of National Intelligence, said Russia, China, Iran and North Korea are engaging in daily cyber attacks against the US. He predicts there will be a major cyber-attack on US critical infrastructure because the 'warning lights are blinking red again.'

"The U.S. intelligence chief warned on Friday that the threat was growing for a devastating cyber assault on critical U.S. infrastructure, saying the "warning lights are blinking red again" nearly two decades after the Sept. 11, 2001, attacks."

"Russia, China, Iran and North Korea are launching daily cyber strikes on the computer networks of federal, state and local government agencies, U.S. corporations, and academic institutions, said Director of National Intelligence Dan Coats."

17.07.18

Euractiv

EU to slam Google with record fine ahead of Juncker US visit

Internet giant Google is facing a $5 billion fine from the European Commission over its Android mobile operating system. CEO of Google Sundar Pichai said, “we’ll appeal the Commission’s decision and take the due process available to us.”

“Google is set to face a record-busting EU antitrust fine this week over its Android mobile operating system but rivals hoping that an order to halt unfair business practices will help them may be disappointed.”

“The European Commission’s decision, delayed by a week by US President Donald Trump’s visit to a NATO summit in Brussels last week, is expected on Wednesday.”

17.07.18

CNN

Russia plans to increase aggression post-World Cup

CNN has reported that Russian intelligence agencies are planning to increase operations targeting Western countries now that the World Cup and the Trump Putin Helsinki summit has ended.

“Russian intelligence agencies are planning to ramp up operations targeting western countries now that the World Cup and the Trump-Putin Helsinki summit have ended, according to sources familiar with intelligence collected by the United Kingdom, the US and other allies.”

“The concern about Russia's intentions preceded this week's meeting between President Donald Trump and Russian President Vladimir Putin.”

19.07.18

SC Media

Russia leads the nation-state attack pack against business

According to a new report by Carbon Black, organisations are ‘woefully unprepared’ to deal with cyber attacks while countries such as Russia, China and the USA are becoming more sophisticated in targeting businesses.

'Russia, China and the USA lead the sophisticated nation-state cyber-attackers that are increasingly targeting businesses, new report reveals.'

"Newly published research suggests that nation-state attacks have evolved to the point where business cannot afford to ignore them."

20.07.18

Nextgov

Trump Administration Plans National Cyber Risk Management Initiative

According to Chris Krebs a US Homeland Security Development official, the Trump administration are creating a 'National Cyber Risk Management' initiative Which seeks to link up several US departments with smaller agencies, so they can collaborate on cybersecurity issues. Krebs said, "It's not just about government working together, it's about industry and government working together."

"The Trump administration is developing a national risk management initiative aimed at tightening communication lines between government and industry about major cyber vulnerabilities, a top Homeland Security Department official said Friday."

"The effort will link Homeland Security and the Energy and Treasury departments with companies in their sectors as well as smaller agencies that regulate or interact with specific sectors that face cyber threats, said Chris Krebs, undersecretary of Homeland Security's cybersecurity and infrastructure protection division."

Privacy

20.07.18

The Wall Street Journal

Facebook Suspends Analytics Firm on Concerns About Sharing of Public User-Data

New concerns over user data sharing has led internet giant Facebook to suspend analytics firm Crimson Hexagon, a company which offers consumer insights and has contracts with Government agencies across the world including Russia and Turkey. According to the Wall Street Journal, Crimson Hexagon has "contracts to analyse public Facebook data for clients including a Russian non-profit with ties to the Kremlin and multiple US government agencies."

"Facebook Inc. suspended another company that harvested data from its site and said it was investigating whether the analytics firm's contracts with the U.S. government and a Russian nonprofit tied to the Kremlin violate the platform's policies."

"Crimson Hexagon, based in Boston, has had contracts in recent years to analyze public Facebook data for those and other contracts, according to people familiar with the matter and federal procurement data."

Internet Inclusion

24.07.18

Nextgov

White House Seeks Input on Reskilling Feds and Upgrading Agency Services

The Trump administration are seeking ways to upgrade their agency services with better technology and reskill their federal employees. The White House invited industry and academia to help create a strategy for this.

"The White House on Monday invited industry and academia to help devise a strategy for building and maintaining a research center for reskilling federal employees and improving citizen services across government."

"The Government Effectiveness Advanced Research, or GEAR, Center would bring together experts from a wide range of fields to come up with innovative ways for agencies to bring outdated services into the 21st century."

25.07.18

SC Media

US Girl Scouts attend camp to spur interest in cyber-security

Girl Scouts in the USA collaborated with Discovery Cube Orange County science center and museum and the Orange County Regional FBI office to create a week-long camp to educated girls in internet safety, cyber-investigations and careers in the FBI.

"The Girl Scouts of the USA joined forces with the Discovery Cube Orange County science center and museum and the Orange County Regional FBI office to create a week-long experience designed to introduce girls to internet safety, cyber-investigations, and careers in the FBI."

"The week-long camp, which ended on 20 July, had the 6th through 8th-grade girls learn how to investigate cyber-crimes fingerprint, conduct victim interviews, collect forensic evidence, interpret blood spatter and extract DNA. The closing event was a mock grand jury trial where the scouts presented the evidence they had gathered earlier."

Pan-Asia

Internet governance

No new items of relevance

Cybersecurity

13.07.18

SC Media

Chinese cyber-espionage group TEMP.Periscope targets Cambodian election

According to FireEye researchers, a cybersecurity company, A Chinese cyber-espionage group called TEMP.Periscope are targeting the Cambodian elections ahead of the countries July 2018 elections.

"A Chinese cyber-espionage group is targeting Cambodian entities ahead of the country's July 2018 elections."

"FireEye researchers spotted the TEMP.Periscope cyber-gang targeting various government entities charged with overseeing the electoral system as well as opposition figures."

14.07.18

Channel NewsAsia

US intel chief warns of devastating cyber threat to US infrastructure

Dan Coats, Director of National Intelligence, said Russia, China, Iran and North Korea are engaging in daily cyber attacks against the US. He predicts there will be a major cyber-attack on US critical infrastructure because the 'warning lights are blinking red again.'

"The U.S. intelligence chief warned on Friday that the threat was growing for a devastating cyber assault on critical U.S. infrastructure, saying the "warning lights are blinking red again" nearly two decades after the Sept. 11, 2001, attacks."

“Russia, China, Iran and North Korea are launching daily cyber strikes on the computer networks of federal, state and local government agencies, U.S.”

19.07.18

SC Media

Russia leads the nation-state attack pack against business

According to a new report by Carbon Black, organisations are ‘woefully unprepared’ to deal with cyber attacks while countries such as Russia, China and the USA are becoming more sophisticated in targeting businesses.

'Russia, China and the USA lead the sophisticated nation-state cyber-attackers that are increasingly targeting businesses, new report reveals.'

“Newly published research suggests that nation-state attacks have evolved to the point where business cannot afford to ignore them.”

19.07.18

Channel NewsAsia

Vietnam says controversial cybersecurity law aims to protect online rights

According to Le Thi Thu Hang, a spokesperson for the Foreign Ministry of Vietnam said the country’s new cybersecurity law will create a ‘safe and healthy cyberspace’ and protect rights online. However, critics argue it grants the Government more power to ‘crackdown on dissent.’

“Vietnam's new cybersecurity law is designed to protect online rights and create a "safe and healthy cyberspace," the foreign ministry said on Thursday, although critics have warned it gives the Communist-ruled state more power to crack down on dissent.”

“Seventeen U.S. lawmakers wrote to the chief executives of Facebook and Google on Wednesday, urging them to resist changes wrought by the new law that require foreign tech firms to store locally personal data on users in Vietnam and open offices there.”

20.07.28

SC Media

Singapore responds quickly to its biggest ever cyber-attack; 1.5 m records stolen

The Singaporean Government have announced that the biggest ever cyber-attack has seen the personal information of 1.5 million people stolen and the Prime Minister Lee Hsien Loong was also targeted. The data stolen includes names, NRIC numbers, addressees, gender, race and date of birth.

"Singapore's government health database has been hacked and the personal information of about 1.5 million people has been stolen, including that of Prime Minister Lee Hsien Loong."

"A joint statement by the Health Ministry and the Ministry of Communications and Information announced: "Investigations by the Cyber Security Agency of Singapore (CSA) and the Integrated Health Information System (IHiS)confirmed that this was a deliberate, targeted and well-planned cyberattack. It was not the work of casual hackers or criminal gangs."

20.07.18

Nextgov

Chinese Hackers Targeted Internet-of-Things During Trump-Putin Summit

Chinese hackers launched a wave of cyber attacks against internet connected devices in Finland a few days before the US and Russian leaders met in Helsinki in a bit to collect audio intelligence from the meeting. According to the report, "Finland is not typically a top attacked country; it receives a small number of attacks on a regular basis."

"Four days before U.S. and Russian leaders met in Helsinki, hackers from China launched a wave of brute-force attacks on internet-connected devices in Finland, seeking to gain control of gear that could collect audio or visual intelligence, a new report says."

"Traffic aimed at remote command-and-control features for Finnish internet-connected devices began to spike July 12, according to a July 19 report by Seattle-based cybersecurity company F5."

Privacy

25.07.18

Channel NewsAsia

8 organisations take part in pilot programme to certify data protection practices

Eight organisations in Singapore that are in the health, lifestyle and financial sectors have announced their plans to help identify businesses that have good data protection practices. Businesses that pass can display the 'Trustmark logo' which gives consumers more confidence and trust in companies.

"Eight organisations from the financial, health and lifestyle sectors will participate in a pilot programme which helps consumers identify businesses that have good data protection practices."

"During the Data Protection Trustmark (DPTM) certification scheme pilot, the organisations - which include, Singtel, DBS Bank, Fullerton Healthcare group and Redmart - will have their data protection practices independently assessed. If they meet the mark, they can use and display the Trustmark logo."

Internet Inclusion

24.07.18

Computer Weekly

Singapore public healthcare sector limits internet use

The public healthcare sector in Singapore have announced their plans to limit the internet access of healthcare workers and require them to use alternative internet workstations, after a major cybersecurity attack crippled healthcare IT systems.

"Healthcare workers who require internet access will have to use separate internet workstations following an unprecedented attack on Singapore's public healthcare system."

"Singapore's public healthcare providers have limited internet use on employees' computers after an unprecedented attack on the country's healthcare IT systems."

24.07.18

Channel NewsAsia

Singapore may use drones to deliver medicine, for security

Future Flight Consortium, a group of 13 members have been tasked with creating a drone programme which will see drones deliver medical supplies to patients and responding to security incidents.

"Drones could be used across hi-tech Singapore to deliver life-saving medical supplies to a patient during an emergency or to respond to a security breach under a new system in development, a private consortium said Tuesday (Jul 24)."

"Future Flight Consortium, a 13-member group, said it had been chosen by the country's civil aviation authority and transport ministry to develop the drone programme."

25.07.18

Channel NewsAsia

Facebook plans innovation hub in China despite tightening censorship

Internet giant Facebook has announced its plans to create an 'innovation hub' in China to help support local start-ups and developers despite the social media site remaining blocked in China.

"Facebook has set up a subsidiary in China and plans to create an "innovation hub" to support local start-ups and developers, the social media company said on Tuesday, ramping up its presence in the restrictive market where its social media sites remain blocked."

"The subsidiary is registered in Hangzhou, home of e-commerce giant Alibaba Group Holding Ltd, according to a filing approved on China's National Enterprise Credit Information Publicity System last week and seen by Reuters on Tuesday."

Rest of the World

Internet governance

18.07.18

The Guardian

Nigeria needs chief information officer at the presidency, says Yele Okeremi

According to Dr. Yele Okeremi**,** the President of Institute of Software Practitioner of Nigeria the Presidency needs a Chief Information Officer who would be responsible for issues like cybersecurity and cyber sovereignty in Nigeria.

"Dr. Yele Okeremi, the president of Institute of Software Practitioner of Nigeria (ISPON), in this interview with ADEYEMI ADEPETUN, spoke on the need for the country to have a chief information officer (CIO) at the Presidency, He also disclosed plans by the body of software practitioners to engage the startup community among other issues. Excerpts."

"It appears that the strong advocacy of ISPON, especially for the patronage of local software has gone down."

Cybersecurity

14.07.18

Channel NewsAsia

US intel chief warns of devastating cyber threat to US infrastructure

Dan Coats, Director of National Intelligence, said Russia, China, Iran and North Korea are engaging in daily cyber attacks against the US. He predicts there will be a major cyber-attack on US critical infrastructure because the 'warning lights are blinking red again.'

"The U.S. intelligence chief warned on Friday that the threat was growing for a devastating cyber assault on critical U.S. infrastructure, saying the "warning lights are blinking red again" nearly two decades after the Sept. 11, 2001, attacks."

"Russia, China, Iran and North Korea are launching daily cyber strikes on the computer networks of federal, state and local government agencies, U.S.

16.07.18

Channel NewsAsia

[Russia says it prevented 25 million cyber attacks, other acts during World Cup]

According to the Russian President, Vladimir Putin, the country stopped nearly 25 million cyber attacks against its information infrastructure during the World Cup. Putin said there were no 'serious incidents' thanks to Russia's tight security and 'people who came to our country really felt they were safe.'

"Russia prevented nearly 25 million cyber attacks and other criminal acts against its information infrastructure related to the soccer World Cup, the Kremlin quoted President Vladimir Putin as saying."

"The comments were made during Putin's meeting with the security council organised for the World Cup on Sunday evening, soon after the tournament ended."

17.07.18

CNN

[Russia plans to increase aggression post-World Cup]

CNN has reported that Russian intelligence agencies are planning to increase operations targeting Western countries now that the World Cup and the Trump Putin Helsinki summit has ended.

"Russian intelligence agencies are planning to ramp up operations targeting western countries now that the World Cup and the Trump-Putin Helsinki summit have ended, according to sources familiar with intelligence collected by the United Kingdom, the US and other allies."

"The concern about Russia's intentions preceded this week's meeting between President Donald Trump and Russian President Vladimir Putin."

19.07.18

SC Media

[Russia leads the nation-state attack pack against business]

According to a new report by Carbon Black, organisations are 'woefully unprepared' to deal with cyber attacks while countries such as Russia, China and the USA are becoming more sophisticated in targeting businesses.

'Russia, China and the USA lead the sophisticated nation-state cyber-attackers that are increasingly targeting businesses, new report reveals.'

"Newly published research suggests that nation-state attacks have evolved to the point where business cannot afford to ignore them."

Privacy

20.07.18

The Wall Street Journal

Facebook Suspends Analytics Firm on Concerns About Sharing of Public User-Data

New concerns over user data sharing has led internet giant Facebook to suspend analytics firm Crimson Hexagon, a company which offers consumer insights and has contracts with Government agencies across the world including Russia and Turkey. According to the Wall Street Journal, Crimson Hexagon has "contracts to analyse public Facebook data for clients including a Russian non-profit with ties to the Kremlin and multiple US government agencies."

"Facebook Inc. suspended another company that harvested data from its site and said it was investigating whether the analytics firm's contracts with the U.S. government and a Russian nonprofit tied to the Kremlin violate the platform's policies."

"Crimson Hexagon, based in Boston, has had contracts in recent years to analyze public Facebook data for those and other contracts, according to people familiar with the matter and federal procurement data."

Internet Inclusion

17.07.18

Channel NewsAsia

Cuba starts rolling out internet on mobile phones

Cuba has announced plans to allow the internet to be rolled out on mobile phones by the end of the year. This is part of a wider strategy to get more people connected to the internet and boost the economy.

"Communist-run Cuba has started providing internet on the mobile phones of select users as it aims to roll out the service nationwide by year-end, in a further step toward opening one of the Western Hemisphere's least connected countries."

"Journalists at state-run news outlets were among the first this year to get mobile internet, provided by Cuba's telecoms monopoly, as part of a wider campaign for greater internet access that new President Miguel Diaz-Canel has said should boost the economy and help Cubans defend their revolution."

18.07.18

Computer Weekly

Deloitte launches EMEA-wide initiative to close cyber security gender gap

Deloitte, a UK-incorporated multinational professional services network has launched a Women in Cyber initiative to help close the gender gap in the cybersecurity sector. Their aim is to create more awareness of the gender gap and help facilitate an environment which encourages women to pursue a career in cybersecurity.

"Professional services organisation Deloitte expands its UK efforts to encourage more women into cyber security to cover the EMEA area."

"Deloitte has launched an EMEA Women in Cyber initiative in an attempt to help close the gender gap in the cyber security sector."

24.07.18

IT News Africa

Afrika Tikkun hosts its first ICT Academy

Afrika Tikkun, a charity in South Africa held its first Information Communication Technology event where experts in the field discussed the ICT skills shortage.

"On Friday, 20 July 2018 Afrika Tikkun hosted its first Information Communication Technology (ICT) Academy launch in partnership with Think Tank under the theme 'let's tackle the ICT skills shortage'."

"The launch event was opened by Group Executive of Partnerships and Marketing, Onyi Nwaneri and Think Tank Managing Director, Tebogo Moleta."

25.07.18

The Guardian

Nigeria's tech startups raise $114.6m in 2017

Startups in Nigeria raised more than $114.6 million in 2017 out of £560 million technology startup investments that entered Africa.

"Country ranks third as investors eye Rwanda, Senegal and Uganda
Out of the $560 million technology startup investments that entered Africa in 2017, Nigeria earned $114.6 million."

"The country ranked third after South Africa and Kenya, which got $167.9 million and $147 million respectively. The three countries accounted for 76 per cent of the total funding that came into the region last year."

25.07.18

The Guardian

SoftTalk, Nigeria owned messaging app for unveiling in Lagos

A new messaging app called SoftTalk is set to be rolled out in Lagos. The hope is that the new app will help create job opportunities and solve local problems.

"SoftTalk, a social media messaging app, developed by a Japan-based Nigerian developer, is set to be unveiled in Lagos."

"The app, which is in the likes of WhatsApp, would help to solve local problems and create job opportunities in the country."

25.07.18

The Guardian

Digify Africa to train 20 graduates on tech talent

DigifyPRO Nigeria, a not for profit organisation that holds intensive boot camps to train aspiring digital professionals has vowed to train 20 Nigerian graduates who are 20-30 years old to provide them with the necessary skills to enter the workforce.

"DigifyPRO Nigeria, a not-for-profit initiative, has concluded plans to train 20 Nigerian graduates between the ages of 20 to 30 years, who are not currently in full-time employment with key skills to enter the digital workplace."

"DigifyPRO is an eight-week intensive digital marketing training programme facilitated by Digify Africa and supported by Facebook, which will involve live briefs workshops/presentations and placement."

Global Institutions

12.07.18

Fifth Domain

NATO summit boosts cybersecurity amid uncertainty

NATO have agreed to create two new bodies, a cyberspace operations center in Belgium and a 'Joint Force Command' in Norfolk, Virginia, to deal with the cybersecurity threat and spread of 'disinformation campaigns.'

"Amid uncertainty over NATO member's defense spending, energy deals with Russia and the very future of the alliance itself, combating Moscow's campaign of digital war quietly emerged as an item of agreement for the 29-state body during a summit in Brussels."

"Consider: Few previous NATO meetings of world leaders have included so much discussion over cybersecurity. In a joint declaration, the word "cyber" appeared 26 times. In what appears to be a first for the alliance, leaders twice mentioned the threat of "disinformation campaigns," that have spread chaos through western countries. The declaration devoted two sections to digital security."

Diary Dates

Women in Tech Council – 20.09.18

London England

5th Annual Industrial Control Cyber Security USA – 18.09.18 – 19.09.18

Sacramento, USA

ISC2 Secure Summit Toronto – 01.10.18

Toronto, Canada

MESCON Cybersecurity Conference (Middle Eastern Security Conference) Muscat – 02.10.18 – 03.10.18

Muscat, Oman