13 June 2018

Synopsis

Scroll to read full summaries with links to news articles.

A large amount of sensitive **US** military data was stolen by the **Chinese Ministry of State Security**. The data taken included information on a missile programme. An investigation into the **cyberattack** is now being undertaken by the **FBI**.

A new **cybersecurity** law has been introduced by **Vietnam** that will give the Government greater control over online content. The law also means that larger tech companies, such as **Facebook**, will have to store **personal data** on Vietnamese people within the country.

The **cybersecurity** sector has been singled out by **ISACA**, an IT association, as a place for increased investment in **China**. The call comes as China continues to transform its digital and tech sectors.

A series of **MEPs** have stated that the **Privacy Shield** agreement between **US** firms and their handling of **EU** citizens' data should be suspended unless America follows the **data protection** agreement.

A panel of experts on **cybersecurity** speaking at **Infosecurity Europe 2018** have stated that private companies and businesses should report all **cyberattack** and crime activity. Under-reporting on the issue has caused problems for Governments and law enforcement who need a better idea of the scale and extent of the issues.

A study has revealed that the **UK** is leading the rest of **Europe** in **tech investment**. Over £5 billion has been invested in the UK whilst near rivals **Germany** and **France** remain on £2.15 billion and £1.55 billion respectively.

The Senate is looking to transform President Trump's **cyber policy** by introducing an array of amendments to the **National Defense Authorisation Act**. Of note within these amendments is one in which President Trump would be required to appoint a White House coordinator on **cybersecurity**.

Researchers at **MIT** have developed new **software transmitters** that scatter data so that an attacker cannot intercept a full packet of data and manipulate it.

Washington State has become the first in the **US** to introduce a **net neutrality** law. The new law replaced the federal regulations imposed after the **FCC** repealed it. It stops home and mobile internet providers from blocking lawful **internet traffic**.

The **Australian Government** has introduced a new taskforce that will aim to deter any **cyberattacks** from occurring during elections. The taskforce follows revelations of many states involving themselves in other nations' **elections**.

A new set of **sanctions** have been given by the **US** Treasury on three Russian individuals and five **Russia** companies. All had allegedly worked with Russian Government intelligence on ways to deploy **cyberattacks** on the US.

A new draft **data protection law** is set to be introduced in **Kenya**. It will aim to set up further safety and security measures for personal data that is held by mobile lenders.

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 June 2018

Table of Contents

Europe

Internet governance

No new items of relevance.

Cybersecurity

08.06.18

Computer Weekly

Businesses must report cyber crime, panel urges

A panel of experts on cybersecurity speaking at Infosecurity Europe 2018 have stated that private companies and businesses should report all cyberattack and crime activity. Under-reporting on the issue has caused problems for Governments and law enforcement who need a better idea of the scale and extent of the issues.

"Under-reporting is a huge problem when it comes to cyber crime, depriving law enforcement organisations of key insights and opportunities to connect criminal activity.

That was the view of a panel of law enforcement and private business representatives at Infosecurity Europe 2018 in London, discussing the importance of partnerships between the two in fighting cyber crime."

11.06.18

European Parliament

Cyber defence: "If one member state is weak, it could harm the others"

In an interview, Urmas Paet, an Estonian member of the European Parliament, stated that more needs to be done by the EU on cybersecurity. He said that Europe faces a risk of increased cyberattacks on military and civilian targets.

"If you were to rate the EU's cyber defence on a scale from one to five, with one being excellent and five being a failure, how would the EU do and why?

Being a little bit optimistic, I would say two. The situation is not bad, but we can do better. The crucial issue is that cyber defence is the responsibility of member states. What the EU can do is to push them to cooperate better, to have more unified structures to combat cybercrime and cyber-attacks, to be prepared to act

if needed; and to provide a platform for cooperation with Nato and third countries. Cybersecurity is international and interlinked so, if one member state is very weak, it could unfortunately harm all the others."

Privacy

13.06.18

Computer Weekly

Dixons Carphone admits 'falling short' on data protection

Following a breach in privacy, Dixons Carphone has issued a warning that personal data for millions of its customers may have been taken. The new privacy breach follows a similar one in 2015 that effected over 3 million people.

"Electrical and telecommunications retailer and services company Dixons Carphone is investigating a cyber intrusion at the company and an attempt to compromise 5.9 million payment cards.

The intrusion was detected in one of the processing systems of Currys PC World and Dixons Travel stores, and also involved more than a million personal data records."

08.06.18

Computer Weekly

European Court hearing into EU-US data transfer system will not happen for at least 18 months

Further delays are expected for the hearing by the ECJ on data transfer systems between the EU and US. The hearing has been raised following the data privacy issues surrounding Facebook and Google.

"The European Court of Justice may not have a hearing into crucial questions about the legality of the EU-US data transfer system for at least 18 months according to a spokesperson for the Court.

On 2nd May the Irish High Court's Judge Caroline Costello sent 11 controversial questions about data transfers to the US, to the EU's highest Court in Luxemburg."

12.06.18

Public Technology

MEPs call for suspension of Privacy Shield unless US complies with data-protection agreement

A series of MEPs have stated that the Privacy Shield agreement between US firms and their handling of EU citizens' data should be suspended unless America follows the data protection agreement.

"Members of the European Parliament's Civil Liberties Committee have called on legislators to suspend the Privacy Shield agreement that governs US firms' handling of EU citizens' data.

MEPs on the committee passed a resolution to call for the suspension of the agreement from 1 September, if the "US fails to comply" with its terms."

Internet Inclusion

12.06.18

Computer Weekly

Mayor Khan bids to make London the world's smartest city

During London's Tech Week, Sadiq Khan, the Mayor of London, officially launched a new initiative to boost technology in the capital. The aim is to improve digital connectivity and city design.

"Using digital and smart city technology to solve urban challenges around air quality, city design and digital connectivity will be the focus of a London-wide initiative launched by London mayor Sadiq Khan this week.

Speaking at the launch of London Tech Week, Khan announced a bid to help address some of London's most pressing problems by turning the capital into the smartest city in the world. His Smarter London Together roadmap comprises more than 20 initiatives designed to reinforce London's credentials as a smart city."

08.06.18

Reuters

[Britain remains top European hub for tech investors: study]

A study has revealed that the UK is leading the rest of Europe in tech investment. Over £5 billion has been invested in the UK whilst near rivals Germany and France remain on £2.15 billion and £1.55 billion respectively.

"Britain remains the leading European destination for international tech investors, with UK tech companies attracting almost three times more venture capital investment than any other European country over the past two years, according to a study on Friday.

London tech firms are contributing to the growth of the nation's digital economy, accounting for over 80 percent of all venture capital money invested into the UK since the 2016 EU referendum vote, it added."

United States of America

Internet governance

No new items of relevance

Cybersecurity

11.06.18

SC Magazine

MIT researchers develop frequency-hopping transmitter that fends off attackers

Researchers at MIT have developed new software transmitters that scatter data so that an attacker cannot intercept a full packet of data and manipulate it.

"Academic researchers say they have invented a transmitter that can secure billions of Internet of Things products by individually scattering each bit of data that a device wirelessly sends out onto different radio frequency channels, thus preventing attackers from intercepting a full packet and manipulating its data.

In essence, the transmitter performs a new-and-improved version of a technique called "frequency hopping," according to a press release issued by the Massachusetts Institute of Technology, where the technology was developed"

11.06.18

SC Magazine

Cybercrime-fighting dogs to the rescue

Canine units are now being trained to sniff out hidden electronic devices in a bid to try and fight cybercrime. A specific chemical compound found in all electronic devices is being made familiar to the dogs.

"In addition to sniffing out drugs, bombs, and other weapons, law enforcement agencies at federal and local levels are training their canine units to assist in fighting cybercrime by sniffing out hidden electronic devices.

The dogs are used to sniff out phones, hard drives, and microSD cards by sniffing for a chemical compound called triphenylphosphine oxide, or TPPO which is used in all electronic devices."

11.06.18

Next Gov

Lawmakers Take Another Shot at Transforming Trump Cyber Policy

The Senate is looking to transform President Trump's cyber policy by introducing an array of amendments to the National Defense Authorisation Act. Of note within these amendments is one in which President Trump would be required to appoint a White House coordinator on cybersecurity.

"Senate lawmakers are taking another stab at shaping the Trump administration's cyber policy, piling cyber amendments that failed in the House onto the Senate version of the National Defense Authorization Act.

One such amendment, authored by Sen. Martin Heinrich, D-N.M., would require President Donald Trump to appoint a White House cybersecurity coordinator, reversing a move by National Security Adviser John Bolton who removed the role in May."

12.06.18

The Hill

Senate confirms Trump Homeland Security cyber pick

Confirmation has been made of Trump's choice of Christopher Krebs as the new Director of Homeland Security National Protection and Programs Directorate. His role includes overseeing the protection of infrastructure from cyberattacks and threats.

"The Senate confirmed President Trump's choice to lead the Department of Homeland Security's cyber and infrastructure protection unit on Tuesday evening.

The Senate confirmed Christopher Krebs in a voice vote Tuesday to serve at the helm of Homeland Security's National Protection and Programs Directorate, or NPPD, roughly four months after Trump nominated him to the post."

13.06.18

Straits Times

US sanctions Russians over cyber attacks

A new set of sanctions have been given by the US Treasury on three Russian individuals and five Russia companies. All had allegedly worked with Russian Government intelligence on ways to deploy cyberattacks on the U.S.

“The US Treasury has imposed sanctions on three Russian individuals and five companies, saying they had worked with Moscow's military and intelligence services on ways to conduct cyber attacks against the US and its allies.

"The entities designated today have directly contributed to improving Russia's cyber and underwater capabilities through their work with the FSB, and therefore jeopardise the safety and security of the United States and our allies," Treasury Secretary Steven Mnuchin said on Monday, referring to Russia's Federal Security Service.”

Privacy

11.06.18

SC Magazine

ENCRYPT Act reintroduced in Congress

A group from the House of Representatives has forwarded a bill to form a national standard encryption for the United States. The plans would overrule current powers held by state and local governmental structures.

“A bipartisan group of representatives has put forth a bill to create a national standard encryption that would supersede any similar standards created on the state or local levels.

Representatives Ted W. Lieu D-Calif., Mike Bishop R-Mich., Suzan DelBene D-Wash. and Jim Jordan R-Ohio reintroduced the Ensuring National Constitutional Rights for Your Private Telecommunications (ENCRYPT) Act. If enacted the bill would ensure a uniform, national policy for the interstate issue of encryption technology.”

Internet Inclusion

11.06.18

ARS Technica

First state net neutrality law took effect today, countering FCC repeal

Washington State has become the first in the US to introduce a net neutrality law. The new law replaced the federal regulations imposed after the FCC repealed it. It stops home and mobile internet providers from blocking lawful internet traffic.

“The State of Washington today became the first US state to impose a net neutrality law that replaces the nationwide regulations repealed by the Federal Communications Commission.

Washington's legislature and governor approved the new law three months ago and arranged for it to take effect as soon as the FCC finalized its repeal. The FCC repeal was finalized today, so Washington's state law has gone into effect.”

Pan-Asia

Internet governance

12.06.18

Reuters

Financial crime task force eyeing binding crypto exchange rules: Japan official

The Financial Action Task Force has stated its intention to introduce rules over exchanges of cryptocurrency. The FATF was created by the G7, with a Japanese official having said that these new binding rules will be phased in by 2019.

"International financial crime-fighting group Financial Action Task Force (FATF) will start discussions later this month on introducing binding rules governing cryptocurrency exchanges, a Japanese government official familiar with the matter said on Tuesday.

The move, spurred by a call in March from financial policymakers from the world's top 20 economies for regulators to monitor cryptocurrencies, would be a step up from the non-binding guidelines currently in place."

07.06.18

Network Asia

Singapore implements AI governance and ethics initiatives

New governance on artificial intelligence has been implemented by the Singapore Government owing to the rapid advancement of technology in the industry. New ethics have also been developed.

"As Singapore develops its digital economy, a trusted ecosystem is key, where industries can benefit from innovations in technology while consumer confidence and understanding can be assured.

It is thus timely to proactively discuss and address ethical issues that may arise from the use of artificial intelligence (AI) and data, as new business models and innovations rapidly develop in the emergent AI space."

12.06.18

Reuters

Vietnam lawmakers approve cyber law clamping down on tech firms, dissent

A new cybersecurity law has been introduced by Vietnam that will give the Government greater control over online content. The law also means that larger tech companies, such as Facebook, will have to store personal data on Vietnamese people within the country.

"Vietnamese legislators approved a cybersecurity law on Tuesday that tightens control of the internet and global tech companies operating in the Communist-led country, raising fears of economic harm and a further crackdown on dissent.

The cyber law, which takes effect on Jan. 1, 2019, requires Facebook (FB.O), Google (GOOGL.O) and other global technology firms to store locally "important" personal data on users in Vietnam and open offices there."

Cybersecurity

11.06.18

SC Magazine

Chinese gov't hackers snag secret missile plans in Navy contractor breach

A large amount of sensitive US military data was stolen by the Chinese Ministry of State Security. The data taken included information on a missile programme. An investigation into the cyberattack is now being undertaken by the FBI.

"Hackers from the Chinese Ministry of State Security who broke into the systems of a contractor working for the U.S. Naval Undersea Warfare Center stole 614GB of sensitive information, including plans for a supersonic anti-ship missile to be launched from a submarine.

The hacks, which occurred in January and February, according to a report in the Washington Post, yielded details on the Sea Dragon missile program, which was created in 2012 to adapt existing military technology to new uses."

07.06.18

Network Asia

New guide to aid auditors in assessing cybersecurity risk in financial statement audits

A publication has been released by the Chartered Accountants Institute in Singapore that handles the cybersecurity risks and issues that the industry faces. The aim is to provide guidance for accountants conducting financial statement audits.

"The Institute of Singapore Chartered Accountants (ISCA) has launched a publication titled 'Cybersecurity Risk Considerations in a Financial Statements Audit" to provide a guide for auditors on assessing cybersecurity risk in a financial statements audit.

This is the first publication in Southeast Asia that provides guidance on cybersecurity risk considerations in a financial statements audit."

12.06.18

China Daily

Cybersecurity efforts boost digital push

The cybersecurity sector has been singled out by ISACA, an IT association, as a place for increased investment in China. The call comes as China continues to transform its digital and tech sectors.

"ISACA, formerly the Information Systems Audit and Control Association, said it sees great strategic importance in China, especially its cybersecurity sector, and has increased its investment in the country by establishing a Beijing office to support the nation's digital transformation and business technology workforce.

"Establishing ISACA's presence in China and supporting the professional community throughout the country marks a significant milestone in ISACA's long-standing relationship with China," said Matt Loeb, CEO of ISACA."

Privacy

12.06.18

SC Magazine

South Korean cryptocurrency exchange hit, sparking drop in bitcoin prices; Ethereum heist nets $20M

Issues over the security and privacy of Coinrail, a South Korean bitcoin exchange company, have come to the fore after just under $40 million was taken in cryptocurrency.

"A cyber assault against a South Korean bitcoin exchange firm Coinrail resulted in steep fall in the cryptocurrency as concerns about its security come into question.

Over the weekend, threat actors made off with about 30 percent of the coins traded on the exchange. Although the firm didn't quantify the value of the heist, a South Korean news agency Yonhap estimated the value of the theft at 40 billion won (US$37.2 million) worth of cryptocurrency."

Internet Inclusion

13.06.18

Arabian Business

Mubadala to launch $400m European tech fund

An investment company based in Abu Dhabi of the UAE has revealed plans to invest $400 million into tech firms in Europe. It has stated its intention to work with European nations, including the UK, to target key regional markets for technological growth.

"Mubadala Investment Company (Mubadala) of Abu Dhabi is set to launch a $400 million fund to invest in European technology companies, the firm announced during London Tech Week, a week-long festival focused on new investment opportunities in the UK.

The fund will be managed by Mubadala Ventures, the firm's venture capital arm, and will target high growth technology companies with global impact. SoftBank Group will also participate as a strategic investor via its SIMI US Holdings I, Inc. subsidiary."

Rest of the World

Internet governance

06.06.18

The Eagle Online

Internet Governance Will Create Robust Internet Economy For Africa – NCC

Internet governance will help boost the African economy, according to the Nigerian Communications Commission. It pushed for investors and stakeholders to involve themselves in the digital sector as a way to help Nigeria grow.

"The Nigeria Communications Commission says internet governance will create a pro-development policy environment and enable the use of the internet as a development engine.

The Executive Vice-Chairman of NCC, Prof. Umar Danbatta, asserted this at the 2018 Nigeria DigitalSENSE Forum series in Lagos with the theme: "Internet Governance: Sustaining Development"."

Cybersecurity

09.06.18

Reuters

Australia forms task force to guard elections from cyber attacks

The Australian Government has introduced a new taskforce that will aim to deter any cyberattacks from occurring during elections. The taskforce follows revelations of many states involving themselves in other nations' elections.

"Australia has established a security task force to guard against cyber attacks and interference in elections, the government said on Saturday, amid concerns foreign powers are meddling in domestic affairs and ahead of five elections next month.

The newly-created Electoral Integrity Task Force will identify and address risks to Australia's electoral process, a Department of Home Affairs spokesperson told Reuters by email."

13.06.18

Straits Times

US sanctions Russians over cyber attacks

A new set of sanctions have been given by the US Treasury on three Russian individuals and five Russia companies. All had allegedly worked with Russian Government intelligence on ways to deploy cyberattacks on the U.S.

“The US Treasury has imposed sanctions on three Russian individuals and five companies, saying they had worked with Moscow's military and intelligence services on ways to conduct cyber attacks against the US and its allies.

"The entities designated today have directly contributed to improving Russia's cyber and underwater capabilities through their work with the FSB, and therefore jeopardise the safety and security of the United States and our allies," Treasury Secretary Steven Mnuchin said on Monday, referring to Russia's Federal Security Service.”

07.06.18

The Guardian

Financial losses to cybercrimes on steady rise to N198b

The Nigerian Minister of Communications, Adebayo Shittu, has stated that cybercrime in the nation has dramatically increased between 2016 and 2017, by some 35%. Current financial losses for the nation are estimated at just shy of $650 million.

“Financial losses to cybercrimes in Nigeria appeared unabated, as the menace increased by 35 per cent between 2016 and 2017, according to the 2017 Nigeria Cyber Security Report. The Minister of Communications, Adebayo Shittu, had in 2016, revealed based on statistics made available to him that the country was losing N127 billion yearly to the menace.

However, latest study, compiled by Serianu Limited and Demadiur Systems Limited, has confirmed a 35 per cent increase in the losses, which currently stood at $649 million (N198.6 billion).”

Privacy

08.06.18

Next Gov

Russia, Too, Is Building a Giant War Cloud

As part of an effort to remain connected to the internet if global connectivity is lost, Russia is developing a giant cloud for completion by 2020. It is part of the Russian military's plan to keep on top of things during possible wartime.

"The Russian military is building a giant cloud, the latest improvement in its ability to keep operating if its connection to the global internet is lost, severed, or hacked."

"Russian Armed Forces will receive a…closed 'cloud' storage for proprietary and confidential information," Izvestia reported this week."

11.06.18

Channel News Asia

Kenya to publish draft data protection bill this month: minister

A new draft data protection law is set to be introduced in Kenya. It will aim to set up further safety and security measures for personal data that is held by mobile lenders.

"Kenya will publish a draft data protection law this month to create safeguards for personal data held by mobile phone-based lenders and others, Minister of Information, Communication and Technology Joe Mucheru said on Monday.

It will specify how data can be stored and shared and will take into account standards set by data protection laws outside Kenya including in the European Union, Mucheru said."

Internet Inclusion

08.06.18

The Guardian

Embracing a digital culture will shape Nigeria's economy – Meflyn Anwana

In Nigeria, the Special Assistant to the Akwa Ibom State Governor on New Media has asked for the region to embrace the digital culture as part of an effort

to boost economic activity in the area. The digital sector will heavily boost employment, the aid believes.

“The Special Assistant to the Akwa Ibom State Governor on New Media, Mrs. Meflyn Anwana, has called on Akwa Ibom people to adopt a digital culture, so as to expedite the emergence of the digital economy envisioned by Governor Udom Emmanuel.

Mrs. Meflyn made the statement at her office in the Akwa Ibom State Government House Press Center, while receiving media practitioner and Secretary of the Coalition of Online Publishers in Akwa Ibom State, Mr. Nelson NseAbasi on Thursday, 7th June 2018.”

Global Institutions

11.06.18

European Parliament

Cyber defence: "If one member state is weak, it could harm the others"

In an interview, Urmas Paet, an Estonian member of the European Parliament, stated that more needs to be done by the EU on cybersecurity. He said that Europe faces a risk of increased cyberattacks on military and civilian targets.

"If you were to rate the EU's cyber defence on a scale from one to five, with one being excellent and five being a failure, how would the EU do and why?

Being a little bit optimistic, I would say two. The situation is not bad, but we can do better. The crucial issue is that cyber defence is the responsibility of member states. What the EU can do is to push them to cooperate better, to have more unified structures to combat cybercrime and cyber-attacks, to be prepared to act if needed; and to provide a platform for cooperation with Nato and third countries. Cybersecurity is international and interlinked so, if one member state is very weak, it could unfortunately harm all the others."

Diary Dates

M-Trends 2018: The Trends Behind Today's Breaches and Cyber Attacks – 21.06.18

London, England

Data Centre Risk Radar – Technical Skills Shortage – 27.06.18

London, England

CyberFirst Briefing with NCSC – 11.07.18

London, England

Women in Tech Council – 20.09.18