08 November 2017

Synopsis

Scroll to read full summaries with links to news articles.

Julian King, European Commissioner for the Security Union has announced at the Financial Times' **Cyber Security Summit** that cybersecurity needs to encompass "the full range of **cybersecurity** challenges which are rooted in, or accelerated by technology"

16 teams of **cybersecurity** researchers from across the academic sphere in **Israel** and **Germany** have combined to create a new cybersecurity accelerator program.

US President **Donald Trump** is set to reaffirm the 2015 **hacking** accord deal with **China** as part of his visit to the country. Trump is also expected to call for closer cyber collaboration in curbing **North Korea's** oppressive regime.

Pro-ISIS **hackers** have managed to access the sites of nearly 800 U.S. schools, displaying **ISIS** messages, a recruitment video and images of former Iraqi President, Saddam Hussein.

A trove of documents exposing secrets of the wealthiest clientele have been leaked, after **Appleby**, an offshore law firm was **hacked**. The files shared by the International Consortium of Investigative Journalists and contained details of nearly 100 multinational corporations including, **Uber**, **Nike** and **Apple**.

Ahsan Iqbal, Minster for Planning and Development has announced that the Government will soon be testing the introduction of **5G** internet connections. He also indicated that he planned to set up research centres for; **cybersecurity**, **big data**, **cloud computing**, **robotics** and **artificial intelligence**.

Singapore's Personal Data Protection Commission has outlined in a consultation document that prohibits, 'the indiscriminate collection of consumers' **personal data**' to avoid personal information being compromised.

Professor **Peter Katjavivi,** Speaker of the **National Assembly of Namibia**, has urged Parliament to speed up the process of enacting a law dealing with

cybercrime. He expressed his concerns at a one-day **cybersecurity** conference in Windhoek.

NATO announced on Monday that they were working on a, 'special doctrine' to help member states collaborate on **cybersecurity**. The Cooperative Cyber Defence Centre of Excellence in Tallinn will help to support NATO's desire to train member states in cybersecurity so that they can better protect their systems.

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

08 November 2017

Table of Contents

Europe

Internet governance

No new items of relevance

Cybersecurity

06.11.17

The Hill

NATO pressing forward on cyber defense, official says

NATO announced on Monday that they were working on a, 'special doctrine' to help member states collaborate on cybersecurity. The Cooperative Cyber Defence Centre of Excellence in Tallinn will help to support NATO's desire to train member states in cybersecurity so that they can better protect their systems.

"NATO is working on a "special doctrine" for cyber operations and taking steps to help member states bolster their cyber defences, an official said Monday."

"Merle Maigre, who directs a NATO-affiliated cyber center headquartered in Tallin, Estonia, outlined the alliance's multi-pronged efforts on cybersecurity during an appearance at the Center for Strategic and International Studies in Washington, D.C."

07.11.17

GOV.UK

The UK and France - A joint approach on digital and cybersecurity

The Digital Minister, Matt Hancock has given a speech at both the Cyber Security: Testing France and the UK's Digital Defences conference in which he praised the close partnership between the two countries on issues such as cybersecurity.

"Good morning, ladies and gentlemen. I am grateful to the Embassy for organising this event. The UK and France have a historic and close partnership and cybersecurity is no exception."

"Whatever challenges we face in the future, with our strong partnership and talent in the UK and France, I know that we will always work to ensure the prosperity of our two countries."

08.11.17

Times of Israel

German-Israel program seeks to boost cybersecurity ecosystem

16 teams of cybersecurity researchers from across the academic sphere in Israel and Germany have combined to create a new cybersecurity accelerator program.

A new German-Israeli partnership launched in Jerusalem this week promises to upgrade cybersecurity collaboration between the two countries.

The Hessian Israeli Partnership Accelerator for Cybersecurity (HIPA)accelerator program will unite 16 teams of cybersecurity experts from the two countries to work on projects related to software, infrastructure and network security. The stated goal of the project is to "trigger the creation of innovation and businesses in cybersecurity in Israel and Germany."

08.11.17

Computer Weekly

Everyone has cybersecurity responsibility, says Euro commissioner

Julian King, European Commissioner for the Security Union has announced at the Financial Times' Cyber Security Summit that cybersecurity needs to encompass "the full range of cybersecurity challenges which are rooted in, or accelerated by technology"

"Everyone has a role to play in cybersecurity, including big market players – but if this is not done voluntarily, legislation may be required, says the European commissioner for security union"

"To tackle the full range of cyber threats, including cyber-enabled terrorism, organised cyber-crime, subversion of democratic processes and manipulation of opinion, there is an urgent need to redefine what is meant by cybersecurity, according to Julian King, European commissioner for security union."

08.11.17

NATO

Doorstep statement

NATO Secretary General Jens Stoltenberg gave a statement in which he announced that cybersecurity is a top priority for the organisation.

"Good morning. Today and tomorrow, defence ministers will take decisions to pave the way for our Summit in July, here in Brussels."

"Those decisions will ensure that NATO continues to adapt for the 21st century so that we can keep our people safe in a more challenging world."

Privacy

06.11.17

ICO.

ICO survey shows most UK citizens don't trust organisations with their data

A survey conducted by the Information Commisioner's Office found that a mere one-fifth of UK citizens trust companies to securely handle their personal data. Only 10% of UK adults whose data has been collected, know what companies do with it.

"The ICO's Deputy Commissioner will be reminding organisations to be transparent with people's personal data after a survey revealed a significant deficit of trust that organisations must address if they want to innovate with personal information."

"The ICO research found that only one fifth of the UK public (20%) have trust and confidence in companies and organisations storing their personal information."

Internet Inclusion

01.11.17

FE news

UK's best young cyber talent representing Britain in 2017 European Cyber Security Challenge

Britain's top 10 cyber enthusiasts are representing the UK in the 2017 European Cyber Security Challenge this week, in Malaga. They will undergo several security challenges such as digital forensics and cryptography.

"Ten of the UK's best cyber enthusiasts are representing Britain in the 2017 European Cyber Security Challenge (ECSC) this week in Malaga. Britain's best cyber talent will be tested in a series of cybersecurity challenges, examining skills from network analysis to digital forensics and cryptography. The UK team will be competing against teams from 15 countries including Spain, Germany, Ireland, Romania and Austria."

United States of America

Internet governance

08.11.17

Politico

[Why Trump is sticking with Obama's China hacking deal]

Donald Trump is set to visit Chinese President Xi Jinping next Wednesday where he will reaffirm the 2015 hacking accord deal with China. Trump is also expected to call for closer cyber collaboration in curbing North Korea's oppressive regime.

"President Donald Trump has broken with a host of Obama-era international agreements, from the Trans-Pacific Partnership to the Paris climate pact — but he's showing every sign of sticking with a 2015 hacking accord with China."

"Last month, the Trump administration quietly reaffirmed the agreement, which Republicans had initially greeted with scepticism. And business groups, cyber researchers and international policy experts say they see little reason for Trump to cancel the deal, especially as he's pressing for China's cooperation in curbing North Korea's increasingly bellicose cyber and nuclear programs."

Cybersecurity

01.11.17

SC Media

[Trump Organization didn't discover shadow subdomains with Russian IPs for four years]

The Trump organisation suffered a serious cyber breach, four years ago, however the hacks had gone undetected until now. New evidence indicates that the perpetrators have ties to Russia.

"A series of shadow subdomains, all with Russian IP addresses and associated with malware campaigns, were created after hackers accessed the domain registration account of the Trump organization and likely went undiscovered until as recently as this week."

"The subdomains could be plainly seen in records of the Trump Organization's domains, according to a report in Mother Jones."

02.11.17

SC Media

Group IB, INTERPOL sign data exchange agreement

Group IB, the company that discovered the BADRABBIT ransomware attacks and INTERPOL have signed a threat-exchange agreement. The deal will see both organisations share cyber intelligence, to help identify threats and combat them accordingly.

"Group IB, the cybersecurity firm that uncovered the Bad Rabbit ransomware attacks in October, inked a threat-exchange agreement with INTERPOL."

"The deal will have the two organizations supply each other with cyberthreat intelligence with Group IB giving information on emerging and known cybersecurity issues and cyberattacks as they take place. This will help expedite the identification of trends and malicious attacks."

03.11.17

Telegraph

US 'to charge six Russian officials' over election hack

The US Justice Department have gathered evidence, identifying individual Russian military and intelligence hackers, who meddled in the US presidential election.

"The US Justice Department has gathered enough evidence to charge six members of the Russian government in the hacking of Democratic National Committee computers before last year's presidential election, the Wall Street Journal reported."

"By identifying individual Russian military and intelligence hackers with charges the US could make it difficult for them to travel, but arresting and jailing them would be unlikely."

06.11.17

Computing

Ransomware attacks will grow significantly in 2018, says Sophos

IT security firm Sophos, has published a new report that argues that Ransomware attacks are going to get increasingly worse, becoming a "fully fledged epidemic" in 2018.

"A report recently published by IT security firm Sophos predicts that ransomware become a fully-fledged epidemic in 2018."

"The report, which took data from clients working with the company between April and October 2017, investigates the security threats that businesses are exposed to today."

07.11.17

Information age

Pro-Isis hackers hijack 800 US schools' sites

Pro-ISIS hackers have managed to access the sites of nearly 800 U.S. schools, displaying ISIS messages, a recruitment video and images of former Iraqi President, Saddam Hussein.

"It has been reported that hackers have managed to access hundreds of websites across the US to post pro-ISIS messages, including images of Saddam Hussein and a recruitment video."

"The hacking group that goes by the name of "Team System Dz" claimed responsibility for the hack, which that took place around 4am EST on Monday (6 November)."

08.11.17

NATO

Doorstep statement

NATO Secretary General Jens Stoltenberg gave a statement in which he announced that cybersecurity is a top priority for the organisation.

"Good morning. Today and tomorrow, defence ministers will take decisions to pave the way for our Summit in July, here in Brussels."

"Those decisions will ensure that NATO continues to adapt for the 21st century so that we can keep our people safe in a more challenging world."

Privacy

01.11.17

BBC News

Hilton Hotels fined for credit card data breaches

Hilton Hotel has been fined $700,000 for mishandling two credit card data breaches relating to hundreds of thousands of customers in 2015. The company was criticised by public officials for its lack of adequate security measures and failure to notify customers in good time.

"Hilton hotels has reached a $700,000 joint settlement with New York and Vermont for a pair of data breaches that were discovered in 2015, including one that exposed more than 350,000 credit card numbers."

"A press release from New York Attorney General Eric Schneiderman states that Hilton Domestic Operating Company did not practice reasonable data security at the time of the breaches, and failed to provide consumers with timely notification, following the incidents."

01.11.17

Guardian

Cybersecurity firm fails to find links between Donald Trump and Russian bank

After allegations of a secret line of communication between Trump and Russia, a US cybersecurity firm, hired by a Russian bank, announced that they found no link between the US and the Russian Bank.

"A US cybersecurity firm hired by a Russian bank to investigate allegations of a secret line of communication with the Trump Organization said on Tuesday there was no evidence so far of substantive contact, email or financial links."

"Mandiant, which is owned by the California-based company FireEye, said it examined internet server logs presented to the bank by media organisations investigating the link."

03.11.17

SC Media

[Another misconfigured Amazon S3 server leaks data of 50,000 Australians]

Amazon has suffered another data leak, after 50,000 Australian employee's personal data was exposed. Full names, passwords, salaries, IDs, Phone numbers and credit card data were all infiltrated.

"Another misconfigured Amazon server has resulted in the exposure of personal data - this time on 50,000 Australian employees that were left unsecure by a third-party contractor."

"This is the country's second largest data breach since the information of 550,000 blood donors was leaked last year."

03.11.17

SC Media

[Hackers find an evil use for SEO]

Hackers using Zenus Panda Banking Trojan have placed hacked sites at the top of Google's search results. This means when consumers search for online banking and personal finance queries, they will arrive at a hacked site, directing them to download a 'word document' which will infect their computer.

"Hackers distributing the Zeus Panda banking trojan have hit upon a new tactic that uses a combination of optimized SEO search terms along with compromised web servers and websites to ensnare their victims."

"Talos Cisco researchers Edmund Brumaghin, Earl Carter and Emmanuel Tacheau detailed the scheme which takes advantage of the fact that so many people simply ask Google for the answer to all the questions that pop up in their daily lives. However, criminals have figured out how to weaponize even innocuous questions like, "how many digits in karur vysya bank account number."

05.11.17

Guardian

Paradise Papers leak reveals secrets of the world elite's hidden wealth

A trove of documents exposing secrets of the wealthiest clientele have been leaked, after Appleby, an offshore law firm was hacked. The files shared by the International Consortium of Investigative Journalists and contained details of nearly 100 multinational corporations including, Uber, Nike and Apple.

"The world's biggest businesses, heads of state and global figures in politics, entertainment and sport who have sheltered their wealth in secretive tax havens are being revealed this week in a major new investigation into Britain's offshore empires."

"The details come from a leak of 13.4m files that expose the global environments in which tax abuses can thrive – and the complex and seemingly artificial ways the wealthiest corporations can legally protect their wealth."

Internet Inclusion

No new items of relevance

Pan-Asia

Internet governance

08.11.17

Politico

Why Trump is sticking with Obama's China hacking deal

Donald Trump is set to visit Chinese President Xi Jinping next Wednesday where he will reaffirm the 2015 hacking accord deal with China. Trump is also expected to call for closer cyber collaboration in curbing North Korea's oppressive regime.

"President Donald Trump has broken with a host of Obama-era international agreements, from the Trans-Pacific Partnership to the Paris climate pact — but he's showing every sign of sticking with a 2015 hacking accord with China."

"Last month, the Trump administration quietly reaffirmed the agreement, which Republicans had initially greeted with skepticism. And business groups, cyber researchers and international policy experts say they see little reason for Trump to cancel the deal, especially as he's pressing for China's cooperation in curbing North Korea's increasingly bellicose cyber and nuclear programs."

Cybersecurity

07.11.17

IndianExpress

Financial institutions concerned by cybersecurity threats: SBI MD

Dinesh Kumar Khara, State Bank of India Managing Director has said that bankers and financial companies were facing increasing difficulty in ensuring their companies were cyber proof.

"Cybersecurity is a cause of concern to every financial company and bankers are facing great difficulty in ensuring it, State Bank of India MD (Risk, IT and Subsidiaries) Dinesh Kumar Khara said on Tuesday."

"Threats are of concern to any financial company. Our employees in the core banking should be informed about and must perceive this threat. Otherwise, they are not vigilant enough," Khara said at a two-day Federation of Indian Chambers of Commerce and Industry (FICCI)-Indian Banks' Association (IBA) Annual Banking Conference (FIBAC) 2017 here."

08.11.17

Indiatoday

[India Today Conclave Next 2017: Experts discuss cybersecurity and its threats]

India's National Cyber Security Coordinator, Gulshan Rai, has called on the Government to increase cyber infrastructure to help India deal with future attacks.

"India Today's TV Managing Editor Rahul Kanwal discusses with a distinguished panel about cyber-security, its threats and where India stands across military, corporate and individual spheres."

"Gulshan Rai, National Cyber Security Coordinator, Prime Minister's Office, addresses some of the concerns regarding the cyber space and how secure it really is. He said that there is potential to enhance the cyber infrastructure. He also referred to WannaCry and Petya ransomware attacks that knocked down servers globally earlier this year. India was also one of the countries affected during the attacks."

Privacy

08.10.17

The Straits Times

[Watchdog seeks stricter protection of NRIC data]

Singapore's Personal Data Protection Commission has outlined in a consultation document that prohibits, 'the indiscriminate collection of consumers' personal data' to avoid personal information being compromised.

"If new rules proposed yesterday kick in, it will become unlawful for mall operators and retailers to collect and use shoppers' NRIC numbers to track parking redemptions, manage their membership accounts or conduct lucky draws."

"Consumers may win the right to refuse to hand over their NRIC details or card, and the onus will be on service providers to use alternative methods such as mobile phone numbers, vehicle numbers or e-mail addresses to identify them."

Internet Inclusion

08.11.17

Daily Pakistan

Pakistan to test 5G service soon, says Ahsan Iqbal

Ahsan Iqbal, Minster for Planning and Development has announced that the Government will soon be testing the introduction of 5G internet connections. He also indicated that he planned to set up research centres for; cybersecurity, big data, cloud computing, robotics and artificial intelligence.

"Minster for Planning and Development Ahsan Iqbal has said after the successful launch of third and fourth generation technology, Pakistan is ready to embrace the 5G platform."

"He stated this while chairing a meeting Joint Stakeholder Meeting on Digital Pakistan in Islamabad, adding that the test of the 5G service will be conducted soon."

Rest of the World

Internet governance

No new items of relevance

Cybersecurity

01.11.17

SC Media

Trump Organization didn't discover shadow subdomains with Russian IPs for four years

The Trump organisation suffered a serious cyber breach, four years ago, however the hacks had gone undetected until now. New evidence indicates that the perpetrators have ties to Russia.

"A series of shadow subdomains, all with Russian IP addresses and associated with malware campaigns, were created after hackers accessed the domain registration account of the Trump organization and likely went undiscovered until as recently as this week."

"The subdomains could be plainly seen in records of the Trump Organization's domains, according to a report in Mother Jones."

07.11.17

New Era

Namibian cyberspace highly vulnerable – Katjavivi

Professor Peter Katjavivi Windhoek-Speaker of the National Assembly, has urged Parliament to speed up the process of enacting a law dealing with cybercrime. He expressed his concerns at a one-day cybersecurity conference in Windhoek.

"Speaker of the National Assembly, Professor Peter Katjavivi, has urged fellow parliamentarians to expedite the process of enacting a law dealing with cybercrime as Namibia continues to rapidly embrace information and communication technology."

"Katjavivi was speaking at the official opening of the one-day cybersecurity conference for members of parliament in Windhoek yesterday."

08.11.17

Times of Israel

German-Israel program seeks to boost cybersecurity ecosystem

16 teams of cybersecurity researchers from across the academic sphere in Israel and Germany have combined to create a new cybersecurity accelerator program.

A new German-Israeli partnership launched in Jerusalem this week promises to upgrade cybersecurity collaboration between the two countries.

The Hessian Israeli Partnership Accelerator for Cybersecurity (HIPA)accelerator program will unite 16 teams of cybersecurity experts from the two countries to work on projects related to software, infrastructure and network security. The stated goal of the project is to "trigger the creation of innovation and businesses in cybersecurity in Israel and Germany."

Privacy

01.11.17

Guardian

Cybersecurity firm fails to find links between Donald Trump and Russian bank

After allegations of a secret line of communication between Trump and Russia, a US cybersecurity firm, hired by a Russian bank, announced that they found no link between the US and the Russian Bank.

"A US cybersecurity firm hired by a Russian bank to investigate allegations of a secret line of communication with the Trump Organization said on Tuesday there was no evidence so far of substantive contact, email or financial links."

"Mandiant, which is owned by the California-based company FireEye, said it examined internet server logs presented to the bank by media organisations investigating the link."

03.11.17

SC Media

Another misconfigured Amazon S3 server leaks data of 50,000 Australians

Amazon has suffered another data leak, after 50,000 Australian employee's personal data was exposed. Full names, passwords, salaries, IDs, Phone numbers and credit card data were all infiltrated.

"Another misconfigured Amazon server has resulted in the exposure of personal data - this time on 50,000 Australian employees that were left unsecure by a third-party contractor."

"This is the country's second largest data breach since the information of 550,000 blood donors was leaked last year."

Internet Inclusion

No new items of relevance

Global Institutions

06.11.17

The Hill

NATO pressing forward on cyber defense, official says

NATO announced on Monday that they were working on a, 'special doctrine' to help member states collaborate on cybersecurity. The Cooperative Cyber Defence Centre of Excellence in Tallinn will help to support NATO's desire to train member states in cybersecurity so that they can better protect their systems.

"NATO is working on a "special doctrine" for cyber operations and taking steps to help member states bolster their cyber defenses, an official said Monday."

"Merle Maigre, who directs a NATO-affiliated cyber center headquartered in Tallin, Estonia, outlined the alliance's multi-pronged efforts on cybersecurity during an appearance at the Center for Strategic and International Studies in Washington, D.C."

08.11.17

NATO

Doorstep statement

NATO Secretary General Jens Stoltenberg gave a statement in which he announced that cybersecurity is a top priority for the organisation.

"Good morning. Today and tomorrow, defence ministers will take decisions to pave the way for our Summit in July, here in Brussels."

"Those decisions will ensure that NATO continues to adapt for the 21st century so that we can keep our people safe in a more challenging world."

Diary Dates

GCCS – 23.11.17-21.11.17

Aero City, New Delhi, India.

IGF 2017 – 18.12.17–21.12.17

Geneva, Switzerland

Manusec Europe – 07.02.18-08.02.18

Munich, Germany

Global Internet and Jurisdiction Conference 2018 – 26.02.18-28.02.18

Ottawa, Canada

RSA – 16.04.18–20.04.18

San Francisco, USA

Africa Internet Summit – 29.04.18-11.05.18

Dakar, Senegal