12 April 2017

Synopsis

Scroll to read full summaries with links to news articles.

IT and Digital Economy ministers from the **G20** met for the first time in **Germany** this week. Following the summit the G20 ministers agreed to ensure **digital access** for all by 2025, though with limited substantive commitments.

Ukraine has engaged with **Chile** on future cooperation on **cybersecurity**. The discussions at the sidelines of the **LAAD 2017** Defence & Security exhibition in **Brazil** are part of Ukraine's hopes of establishing greater cooperation with South American countries.

The European Parliament has supported a resolution that calls on the European Commission to compel the Trump administration to guarantee privacy safeguards enshrined in the **EU-US Privacy Shield**.

In the **United States** the Senate Commerce Committee has supported the passage of a bill designed to deliver **cybersecurity** advice to small business from the **National Institute of Standards and Technology**.

FCC chairman **Ajit Pai** has made several comments this week relating to **net neutrality** and **digital privacy**. On net neutrality, Pai outlined his desire to repeal existing regulation in favour of voluntary commitments. Pai has also stated in an op-ed with FTC Chair Maureen Ohlhausen that strict privacy rules are not required for the Internet Service Providers as there are high levels of competition in the wireless broadband market.

President **Donald Trump** and Chinese President **Xi Jinping** have concluded their first summit, in which President Xi is believed to have pushed for agreements on trade and future **cybersecurity** cooperation.

In the **Phillipines** the Government has been urged by a leading IT expert to invest futher in **cybersecurity** as part of its existing plans to widen the country's national broadband infrastructure.

The Information Technology and Telecommunication Ministry in **Pakistan** has announced that within the next three months it will introduce for the first time a **Data Protection Act** to protect the privacy of citizens both online and offline.

Kaspersky have revealed this week that an unnamed **Brazilian Bank** has suffered a serious **security breach**, resulting in the seizure of the Bank's website and corporate email account.

Fortinet Network Security Academy have announced plans to provide further cybersecurity **training** in both **Australia** and **New Zealand** in a bid to address a growing shortage of skilled **cybersecurity** professionals.

ICANN announced a 12 month postponement of the next Country Code Names Supporting Organization Review following concerns from the membership relating to bandwidth.

IEEE Global Internet Policy Monitor

12 April 2017

Table of Contents

Disclaimer: Please note that this monitor is a summary of news sources and does not reflect the official views of IEEE.

Europe

Internet governance

07.04.17

IP Watch

[G20 IT Ministers Want Access For All, Commit To Conflicting Objectives](#)

IT and Digital Economy ministers from the G20 have met for the first time in Germany this week. Following the summit the G20 ministers agreed to ensure digital access for all by 2025, though with limited substantive commitments.

"The Group of 20 (G20) ministers responsible for the digital economy today called for further efforts to advance access to the internet for everyone and close the digital gaps that still exist. Gathered in Dusseldorf, Germany, for the two-day IT related preparatory conference for the G20 Summit in Hamburg in July, the ministers signed a declaration on "Shaping the Digitalisation for an Interconnected World." It was the first time that ministers for digital economy met in the G20 format."

Cybersecurity

05.04.17

Security Brief

[IoT security in danger of being ignored, says Trend Micro](#)

Trend Micro have called for greater attention to be paid to the cybersecurity of IoT devices, arguing that recent Mirai and Dyn botnet attacks have highlighted the need for discussion in this area.

"Security in Internet of Things (IoT) devices has been highlighted by the recent Mirai and Dyn botnet attacks - and Trend Micro says that most of those devices come with preset, easy passwords and inactivated security.

Organisations that install the technology also suffer by not ever using reinforced configurations, which means hackers can exploit significant holes, Trend Micro says."

06.04.17

Interfax Ukraine

[**Ukraine offers cooperation in UAV creation, cyber security to Chile**](#)

Ukraine have engaged with Chile on future cooperation on cybersecurity. The discussions at the sidelines of the LAAD 2017 Defence & Security exhibition in Brazil is part of Ukraine's hopes of establishing greater cooperation with South American countries.

"Ukraine is interested in establishing defense cooperation with Latin America countries. Chile is considered among potential partners.

The press service of Ukroboronprom State Concern reported that the opportunities of establishing cooperation with Chili were discussed during negotiations of a Ukrainian delegation with Defense Minister of Chile Jose Antonio Gomez at the LAAD 2017 Defence & Security exhibition in Rio de Janeiro (Brazil)."

10.04.17

Reuters

[**British lender Wonga warns customers of personal data hack**](#)

The UK lender Wonga has suffered a major cybersecurity breach in both the UK and Poland. The hack is believed to have led to the disclosure of personal data of 270,000 past and present customers

"British lender Wonga has warned customers in Britain and Poland that their personal data may have been stolen in the latest major corporate security breach.

Cyber attacks have recently affected other British banks, businesses and institutions, including Tesco Bank, Lloyds, Talk-Talk, and the National Health Service"

Privacy

06.04.17

EURACTIV

[MEPs want Commission to toughen up Privacy Shield under Trump](#)

The European Parliament has supported a resolution that calls on the European Commission to compel the Trump administration to guarantee privacy safeguards enshrined in the EU-US Privacy Shield.

"The European Parliament wants the European Commission to 'Trump-proof' the Privacy Shield data sharing agreement between the EU and the United States after the new US administration threatened to roll back some privacy safeguards.

A slender majority of MEPs approved a resolution today (6 April) asking the Commission to force the Trump administration to guarantee privacy safeguards and give the European Parliament access to documents detailing how the Privacy Shield agreement has been enforced by US authorities during a legal review in September. The resolution passed with 306 votes in favour and 240 against."

06.04.17

SC Magazine

[Europe less concerned about privacy than its global counterparts](#)

A new report has found that European businesses are less concerned with data privacy than companies elsewhere in the world like the US, Brazil and China. Companies in the EU also found data privacy to be less of a competitive differentiator than companies in Asia and North & South America.

"European countries are less concerned with privacy in comparison to other countries such as Canada, the US, Brazil, China and India.

According to research from Forrester, the way companies handle and protect consumer data privacy is more than a compliance issue. It's important for customer insights (CI) teams to have an understanding of global privacy concerns since they affect the business' ability to collect, store and use customer data."

Internet Inclusion

No new items of relevance

United States of America

Internet governance

07.04.17

IP Watch

[G20 IT Ministers Want Access For All, Commit To Conflicting Objectives](#)

IT and Digital Economy ministers from the G20 have met for the first time in Germany this week. Following the summit the G20 ministers agreed to ensure digital access for all by 2025, though with limited substantive commitments.

"The Group of 20 (G20) ministers responsible for the digital economy today called for further efforts to advance access to the internet for everyone and close the digital gaps that still exist. Gathered in Dusseldorf, Germany, for the two-day IT related preparatory conference for the G20 Summit in Hamburg in July, the ministers signed a declaration on "Shaping the Digitalisation for an Interconnected World." It was the first time that ministers for digital economy met in the G20 format."

Cybersecurity

05.04.17

The Hill

[Senate panel advances small business cybersecurity bill](#)

The Senate Commerce Committee has supported the passage of a bill designed to deliver cybersecurity advice to small business from the National Institute of Standards and Technology.

"The Senate Commerce Committee advanced a bill Wednesday aimed at boosting resources to help small businesses protect their digital assets from cyber threats.

Sen. Brian Schatz (D-Hawaii) introduced the bill last week, with a bipartisan group of senators including committee chair John Thune (R-S.D.) and ranking member Bill Nelson (D-Fla.) sponsoring."

05.04.17

Security Brief

[IoT security in danger of being ignored, says Trend Micro](#)

Trend Micro have called for greater attention to be paid to the cybersecurity of IoT devices, arguing that recent Mirai and Dyn botnet attacks have highlighted the need for discussion in this area.

"Security in Internet of Things (IoT) devices has been highlighted by the recent Mirai and Dyn botnet attacks - and Trend Micro says that most of those devices come with preset, easy passwords and inactivated security.

Organisations that install the technology also suffer by not ever using reinforced configurations, which means hackers can exploit significant holes, Trend Micro says."

Privacy

05.04.17

Ars Technica

[FCC chairman says US broadband market too competitive for strict privacy rules](#)

The FCC chairman Ajit Pai has stated in an op-ed with FTC Chair Maureen Ohlhausen that strict privacy rules are not required for US Internet Service Providers as there are high levels of competition in the wireless broadband market.

"Federal Communications Commission Chairman Ajit Pai and his counterpart at the Federal Trade Commission today argued that strict privacy rules for ISPs aren't necessary in part because the broadband market is more competitive than the search engine market.

Internet users who have only one choice of high-speed home broadband providers would probably scoff at this claim. But an op-ed written by Pai and Acting FTC Chair Maureen Ohlhausen ignored the lack of competition in home Internet service, focusing only on the competitive wireless broadband market. Because of this competition, it isn't fair to impose different rules on ISPs than on websites, they wrote."

06.04.17

EURACTIV

[MEPs want Commission to toughen up Privacy Shield under Trump](#)

The European Parliament has supported a resolution that calls on the European Commission to compel the Trump administration to guarantee privacy safeguards enshrined in the EU-US Privacy Shield.

"The European Parliament wants the European Commission to 'Trump-proof' the Privacy Shield data sharing agreement between the EU and the United States after the new US administration threatened to roll back some privacy safeguards.

A slender majority of MEPs approved a resolution today (6 April) asking the Commission to force the Trump administration to guarantee privacy safeguards and give the European Parliament access to documents detailing how the Privacy Shield agreement has been enforced by US authorities during a legal review in September. The resolution passed with 306 votes in favour and 240 against."

06.04.17

Info World

[Twitter sues the US government for demanding it unmask an 'alt' account](#)

Twitter has sued the Government after a request was made to disclose the identity of the @alt_uscis which has repeatedly criticised government policy on immigration and like similar alt accounts is believed to be run by employees of the Government.

"Twitter is suing the U.S. Department of Homeland Security and alleging the government is misusing an investigative tool as part of an internal witch-hunt to uncover who is behind a Twitter account critical of the immigration service.

The lawsuit, filed on Thursday in California, comes on the heels of a report that visitors to the U.S. could soon be routinely asked to hand over email and social media account passwords to the immigration service."

Internet Inclusion

07.04.17

Ars Technica

[**FCC chair wants to replace net neutrality with "voluntary" commitments**](#)

The FCC chairman Ajit Pai has outlined his desire to repeal existing net neutrality regulation in favour of voluntary commitments. Another of Mr Pai's proposals to reverse existing net neutrality regulations would be to move responsibility for the issue to the Federal Trade Commission.

"Federal Communications Commission Chairman Ajit Pai reportedly met with broadband industry lobby groups this week to discuss his plans for eliminating net neutrality rules.

Instead of the FCC continuing to enforce net neutrality rules, Pai "wants Internet service providers to voluntarily agree to maintain an open Internet," [Reuters reported yesterday](#), citing three sources briefing on the meeting."

Pan-Asia

Internet governance

07.04.17

IP Watch

G20 IT Ministers Want Access For All, Commit To Conflicting Objectives

IT and Digital Economy ministers from the G20 have met for the first time in Germany this week. Following the summit the G20 ministers agreed to ensure digital access for all by 2025, though with limited substantive commitments.

"The Group of 20 (G20) ministers responsible for the digital economy today called for further efforts to advance access to the internet for everyone and close the digital gaps that still exist. Gathered in Dusseldorf, Germany, for the two-day IT related preparatory conference for the G20 Summit in Hamburg in July, the ministers signed a declaration on "Shaping the Digitalisation for an Interconnected World." It was the first time that ministers for digital economy met in the G20 format."

08.04.17

Strait Times

Xi-Trump summit: China suggests new platform for dialogue, tackles thorny issues

President Donald Trump and Chinese President Xi Jinping have concluded their first summit, in which President Xi is believed to have pushed for agreements on trade and future cybersecurity cooperation.

"Thorny issues such as trade and cybersecurity were raised by Chinese President Xi Jinping on the first day of his summit with US counterpart Donald Trump in Florida, according to the South China Morning Post, as well as a means for regular dialogue.

Xi opened the door for new dialogue between China and the US in a number of difficult areas, said the daily, adding that China's leader had been warmly welcomed "as a friend" by Trump, who had accepted an invitation to visit China later this year (2017)."

Cybersecurity

05.04.17

Security Brief

[IoT security in danger of being ignored, says Trend Micro](#)

Trend Micro have called for greater attention to be paid to the cybersecurity of IoT devices, arguing that recent Mirai and Dyn botnet attacks have highlighted the need for discussion in this area.

"Security in Internet of Things (IoT) devices has been highlighted by the recent Mirai and Dyn botnet attacks - and Trend Micro says that most of those devices come with preset, easy passwords and inactivated security.

Organisations that install the technology also suffer by not ever using reinforced configurations, which means hackers can exploit significant holes, Trend Micro says."

08.04.17

Manilla Times

[IT expert urges govt to invest in cybersecurity](#)

The Phillipines Government has been urged by a leading IT expert to invest futher in cybersecurity as part of its existing plans to widen the country's national broadband infrastructure.

"The Duterte administration's priority program, the creation of a national broadband infrastructure, has drawn the support of one of the world's top PC makers who urged the government to invest on technology to ensure data security and protect confidential information from cyber criminals.

The Department of Information and Communications Technology (DICT), the lead agency charged with implementing the program, has been at the forefront these efforts."

10.04.17

Reuters

[Cyber attack on Union Bank of India similar to Bangladesh heist: WSJ](#)

The Wall Street Journal has reported that a cyber attack on the Union Bank of India bares significant similtarities to the $81million attack on the central bank of

Bangladesh. The attacks both used malware entrenched in email attachments to gain access to the SWIFT messaging system.

"A cyber attack on Union Bank of India last July began after an employee opened an email attachment releasing malware that allowed hackers to steal the state-run bank's data, the Wall Street Journal reported on Monday.

The attempt closely resembled the cybertheft last year of more than $81 million from the Bangladesh central bank's account at the New York Federal Reserve, the paper reported."

11.04.17

Reuters

[China draft cyber law mandates security assessment for outbound data](#)

The Chinese cyber authority has announced through a new draft law that companies exporting data abroad will now undergo yearly security assessment. This could potentially have significant consequences for international businesses as data with economic, technological or scientific value whose transfer could pose a threat to security or public interest will be banned from leaving China under the law.

"China's top cyber authority on Tuesday released a draft law that would require firms exporting data to undergo an annual security assessment, in the latest of several recent safeguards against threats such as hacking and terrorism.

Any business transferring data of over 1000 gigabytes or affecting over 500,000 users will be assessed on its security measures and on the potential of the data to harm national interests, showed the draft from the Cyberspace Administration of China (CAC)."

Privacy

05.04.17

Pakistan Today

[IT ministry to introduce DPA within three months](#)

The Information Technology and Telecommunication Ministry in Pakistan has announced that within the next three months it will introduce for the first time a Data Protection Act to protect the privacy of citizens both online and offline.

"Data Protection Act (DPA) is likely to be introduced in the country within three months as the Information Technology and Telecommunication Ministry is taking all possible measures to protect the rights of internet users.

Information Technology and Telecommunication Minister Anusha Rahman on Wednesday said her ministry has been trying hard to introduce the Data Protection Act to safeguard the online and the offline rights of internet users in the country. And, consultations with all relevant stakeholders are in process, she added."

Internet Inclusion

No new items of relevance

Rest of the World

Internet governance

07.04.17

IP Watch

G20 IT Ministers Want Access For All, Commit To Conflicting Objectives

IT and Digital Economy ministers from the G20 have met for the first time in Germany this week. Following the summit the G20 ministers agreed to ensure digital access for all by 2025, though with limited substantive commitments.

"The Group of 20 (G20) ministers responsible for the digital economy today called for further efforts to advance access to the internet for everyone and close the digital gaps that still exist. Gathered in Dusseldorf, Germany, for the two-day IT related preparatory conference for the G20 Summit in Hamburg in July, the ministers signed a declaration on "Shaping the Digitalisation for an Interconnected World." It was the first time that ministers for digital economy met in the G20 format."

Cybersecurity

05.04.17

Security Brief

IoT security in danger of being ignored, says Trend Micro

Trend Micro have called for greater attention to be paid to the cybersecurity of IoT devices, arguing that recent Mirai and Dyn botnet attacks have highlighted the need for discussion in this area.

"Security in Internet of Things (IoT) devices has been highlighted by the recent Mirai and Dyn botnet attacks - and Trend Micro says that most of those devices come with preset, easy passwords and inactivated security.

Organisations that install the technology also suffer by not ever using reinforced configurations, which means hackers can exploit significant holes, Trend Micro says."

05.04.17

SC Media

[Brazilian bank hacked, loses control of its online presense](#)

Kaspersky have revealed this week that an unnamed Brazilian Bank has suffered a serious security breach, resulting in the seizure of the Bank's website and corporate email account.

"A Brazilian bank had all of its 36 domains and other online assets seized by hackers who then used the pages to push malware onto the banks customers.

The attack was first noticed in October 2016 when two Kaspersky Labs researchers, Fabio Assolini and Dmitry Bestuzhev, realized that what they initially believed was a basic site hijacking was in fact a case where someone had taken control of the site's index file. The malicious actors then injected an iframe that redirected the bank's customers and other visitors to another website where they were exposed to a zipped Java plugin containing malware. At the same time this gave them control of the bank's corporate email and DNS."

06.04.17

Interfax Ukraine

[Ukraine offers cooperation in UAV creation, cyber security to Chile](#)

Ukraine have engaged with Chile on future cooperation on cybersecurity. The discussions at the sidelines of the LAAD 2017 Defence & Security exhibition in Brazil is part of Ukraine's hopes of establishing greater cooperation with South American countries.

"Ukraine is interested in establishing defense cooperation with Latin America countries. Chile is considered among potential partners.

The press service of Ukroboronprom State Concern reported that the opportunities of establishing cooperation with Chili were discussed during negotiations of a Ukrainian delegation with Defense Minister of Chile Jose Antonio Gomez at the LAAD 2017 Defence & Security exhibition in Rio de Janeiro (Brazil)."

11.04.17

Security Brief

[A triumph for cyber security: New Zealand's CERT team has finally been launched](#)

As part of the Government's Cyber Security Strategy and Action Plan a Computer Emergency Response Team has been established in New Zealand. The CERT team will receive $22.2 million over the next four years.

"New Zealand's Computer Emergency Response Team (CERT NZ) has finally been launched this afternoon, prompting a new era in the battle against cyber threats.

CERT NZ will be the first port of call for New Zealanders who wish to report cyber incidents."

Privacy

No new items of relevance

Internet Inclusion

10.04.17

Security Brief

[Fortinet to launch ANZ security training course to address skills shortage crisis](#)

Fortinet Network Security Academy have announced plans to provide further cybersecurity training in both Australia and New Zealand in a bid to address a growing shortage of skilled cybersecurity professionals.

"Fortinet is venturing into the cybersecurity training and education market to help address the skills shortage crisis. The company is offering its Network Security Expert (NSE) training and certification program, completely free of charge.

The new program is running through Fortinet's Network Security Academy. Its first ANZ base is at TAFE SA in South Australia. It has already started teaching the program to local cybersecurity experts."

Global Institutions

06.04.17

ICANN

Deferral of Country Code Names Supporting Organization Review

ICANN have announced a 12 month postponement of the next Country Code Names Supporting Organization Review following concerns from the membership relating to bandwidth.

"The ccNSO Review, scheduled to start in August 2017, is proposed to be deferred by 12 months, in response to community concerns about bandwidth.

As per ICANN's Bylaws, Article 4, Section 4.4 (a), organizational reviews, such as the ccNSO Review, 'shall be conducted no less frequently than every five years, based on feasibility as determined by the Board.'"

07.04.17

ICANN

Fifteen Candidates Have Been Selected for NextGen@ICANN59

ICANN has announced the 15 candidates selected from African Universities to attend the ICANN59 Policy Forum.

"ICANN announced today that 15 individuals from various African universities have been selected to attend the ICANN59 Policy Forum, which is being held in Johannesburg, South Africa, from 26-29 June 2017. These students are studying a wide range of topics, including policy, computer science, technology, law and communications. Five additional selectees who attended a previous ICANN meeting as NextGenners will now serve as ambassadors for these newcomers."

10.04.17

ICANN

Survey to Contribute Your Views to the Independent Assessment of the Ombudsman Office

ICANN have launched a new survey to collect views and options of the body's Ombudsmans Office. ICANN has launched the survey in response to previous

recommendations emanating from the Second Accountability and Transparency Review.

"Have you ever interacted with ICANN's Office of the Ombudsman? Do you have thoughts on areas for improvement? Please take the survey to contribute to the current Ombudsman Assessment.

This assessment of the ICANN Ombudsman Office was initiated in response to Recommendations from the Second Accountability and Transparency Review and the community-led WorkStream 2."

Diary Dates

Building the European data economy – **10.01.17-26.04.17**

ITU Council 2017 – **15.05.17 – 25.05.17**

Geneva, Switzerland

Africa Internet Summit (AIS) 2017 – **29.05.17 – 02.06.17**

Nairobi, Kenya

European Dialogue on Internet Governance – **06.06.17-07.06.17**

Tallinn, Estonia

World Summit on the Information Society Forum (WSIS) 2017 – **12.06.17 – 16.06.17**

Geneva, Switzerland

16th European Conference on Cyber Warfare and Security ECCWS – **29.06.17-30.06.17**

Dublin, Ireland

ITU WTDC-17 – **09.10.17 – 20.10.17**

Buenos Aires, Argentina

IGF 2017 – **18.12.17 – 21.10.17**

Geneva, Switzerland