31 May 2017

Synopsis

Scroll to read full summaries with links to news articles.

The **European Union** has agreed to provide €120million from the bloc's budget to provide free **Wi-Fi** to 8,000 local areas currently without internet coverage, with a potential deadline of 2020.

Lithuania's President will travel to **Estonia** at the start of June to discuss bilateral relations and to launch an event to promote a pan-European dialogue on **Internet governance**.

A new report by the **Potomac Institute for Policy Studies** has found that the **Netherlands** have made significant steps in adapting to **cyber threats**, though notes that there remains issues regarding decision-making.

A new bill has been introduced in the Senate by a bipartisan alliance to create a **bug bounty** program for the **Department of Homeland Security**.

Major technology companies **Facebook**, **Google** and **Microsoft** have joined with other firms to lobby Congress to revise the existing US laws on **foreign surveillance** so that greater attention is paid to **digital privacy**.

Elsewhere the **Department of Justice** has asked Congress to provide it with the necessary powers to serve **warrants** against data held abroad, allowing the department to forgo current national jurisdiction rules in the pursuit of **cybercriminals** and terrorists.

Ahead of its introduction this week the **Chinese** Government have issued a statement defending its controversial new **cyber law**, stating that its intention is not to impact the Chinese dealings of international businesses.

The **Data Security Council** of **India** has announced that it will look to abandon **passwords** as a security measure in favour of other technological tools currently under consideration.

Details have emerged indicating that in a bid to avoid the impact of the **WannaCry ransomware** attack five **Australian** hospitals have frozen staff members out of their computer systems through the improper installation of **security patches**.

The **African Union** has unveiled a new set of **cybersecurity** guidelines which are hoped will better protect the continent from **cyberattacks** in the future that bare similarities to this month's **WannaCry** ransomware attack.

Ethiopia's government has closed its citizen's access to the internet in a bid to prevent exam paper leaks that affected last years end of year exams for students in the 12th grade. This is the third time in the last 12 months that the government has **suspended internet access**.

Digital Europe has published its response to the joint **ENISA**, EU Commission consultation on **ICT security certification**. In its submission the group indicated that greater attention be paid to the processes of security certification so as to retain flexibility in applying to products and services.

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

31 May 2017

Table of Contents

Europe

Internet governance

30.05.17

Telecompaper

Polish ministry's think tank consults on internet governance

The Polish Government's Ministry of Digitisation has published the interim findings of its experts council regarding internet governance and net neutrality, as part of an ongoing national discussion regarding the role of state and non-state actors in internet regulation.

"The Polish Ministry of Digitisation has published on its web site the interim results of the work of the Council of Digitisation (RdC) on internet governance and network neutrality. RdC does not prepare legal acts but only reports and recommends. It is a think-tank whose members support the knowledge and experience of the Ministry of Digitisation and Committee of the Council of Ministers for Digitisation. It gives its opinion on strategic documents and other documents related to digitisation, connectivity and development of the information society. RdC will prepare recommendations for Poland's position within international ongoing discussion on the above issues. RdC is inviting the public for comments until 9 June."

31.05.17

Baltic Times

Lithuania's president to travel to Estonia for state visit

Lithuania's President will travel to Estonia at the start of June to discuss bilateral relations and to launch an event to promote a pan-European dialogue on Internet governance.

"During meetings with Estonia's leaders on June 5-6, Grybauskaite will discuss bilateral relations, the enhancement of the Baltic states' security, defense and deterrence, and the implementation of regional strategic projects in the fields of energy and transport, as well as other topical EU issues, the Lithuanian President's Office, said.

According to the press release, Lithuania and Estonia neighbor an unpredictable Russia and face its direct conventional and unconventional threats. Both states are therefore bound by their all-out efforts to strengthen military, energy,

information and cyber security of the region, to implement effectively NATO's deterrence and defense measures, to synchronize the Baltic power grid with Western European network, to protect strategic infrastructure from cyber attacks, and to prevent the spread of lies and propaganda."

Cybersecurity

24.05.17

SC Media

Netherlands nearly up to speed in cyber-security, says readiness report

A new report by the Potomac Institute for Policy Studies has found that the Netherlands have made significant steps in adapting to cyber threats, though notes that there remains issues regarding decision-making.

"The Netherlands has made great strides in implementing its cyber-security strategy, says latest CRI report, but still needs to address issues with funding and decision-making.

An assessment of The Netherlands' preparations for cyber-crime and cyber-warfare has found the country is prepared on several fronts but there is still room for improvement."

31.05.17

Politico

German cyber chief: Election hack 'could happen to us'

The head of Germany's cybersecurity authority Arne Schönbohm has warned that the country's autumn elections could fall victim to the same Russian hacking attempts that affected the US and French presidential elections in the last year.

"The German elections could be affected by hacking just like the U.S. presidential elections last year, the head of the Germany's cyber authority said today.

"Of course, the same could happen to us," said Arne Schönbohm, president of the Federal office for Information Security."

Privacy

No new items of relevance

Internet Inclusion

30.05.17

Euractiv

EU agrees to fund free Wi-Fi for European towns with no internet coverage

The European Union has agreed to provide €120million from the bloc's budget to provide free Wi-Fi to 8,000 local areas currently without internet coverage, with a potential deadline of 2020.

"European Union legislators agreed yesterday (29 May) to set aside €120 million to provide free wireless internet connections by 2020 to up to 8,000 municipalities in the EU in areas with no internet coverage.

The initiative will be funded from the current €1 trillion EU budget, which runs from 2014 to 2020. Towns will have to apply to get the funds "in principle on a first-come, first-served basis," although some geographical balance between the EU's 28 member states will be sought, said the Maltese EU Presidency, which brokered the agreement."

United States of America

Internet governance

26.05.17

SC Media

US DoJ asks Congress for power to serve international data warrants

Elsewhere the Department of Justice has asked Congress to provide it with the necessary powers to serve warrants against data held abroad, allowing the department to forgo current national jurisdiction rules in the pursuit of cybercriminals and terrorists.

"Data centres in the UK could soon find themselves served with warrants by US law enforcement authorities. The US Department of Justice is looking to free itself from the burdens of national jurisdiction, so it can effectively pursue international crime.

The DoJ is asking the US Congress whether it can start making reciprocal international agreements to enable it to serve warrants on data held in other countries – a move that could upset tech companies."

Cybersecurity

26.05.17

Next Gov

U.S. embassies lag on digital security

A new audit of US cybersecurity at its foreign embassies and consulates has found that not enough is being done to protect computer networks.

"Information security staff in U.S. embassies and consulates are falling down on the job, according to an inspector general's audit out this week.

State's internal auditors reviewed information security at 51 overseas posts between fiscal years 2014 and 2016 and found one-third of them, 17 posts, weren't performing basic tasks such as regularly analyzing information systems or reviewing email systems, user libraries, servers and hard drives for indications of inappropriate activity."

30.05.17

SC Media

Bug Bounty program proposed for DHS

A new bill has been introduced in the Senate by a bipartisan alliance to create a bug bounty program for the Department of Homeland Security.

"Two U.S. senators have introduced a bill that would create a bug bounty program for the Department of Homeland Security (DHS), but industry experts warned those participating in the program need to be properly vetted.

Senators Maggie Hassan, D-N.H., and Rob Portmann, R-Ohio, late last week introduced the Hack Department of Homeland Security Act that aims to leverage the work of white-hat hackers to help strengthen DHS by pointing out failure points in the code that runs the agency's website and computer network. Similar programs have been used not only in the private sector, but the Department of Defense instituted the Hack the Pentagon, Hack the Air Force and Hack the Army. In each case white hats found dozens of bugs enabling these services to tighten up their security."

30.05.17

The Hill

Bill aims to boost cybersecurity efforts in Asia-Pacific region

Mac Thornberry the Republican Chairman of the House Armed Services Committee has introduced new legislation to require the US Department of Defence to provide greater information on cybersecurity efforts in the Indo-Asia-Pacific Region.

"A House committee chairman has introduced legislation aimed at increasing cyber cooperation with allies in the Indo-Asia-Pacific region.

The bill, introduced by House Armed Services Committee Chairman Mac Thornberry (R-Texas), would require the Pentagon to report to Congress on how to enhance cyber defense efforts and counter propaganda coming from China, Russia and North Korea."

Privacy

24.05.17

SC Media

Apple transparency report shows increased U.S. national security requests

Apple have revealed an increase in FISA orders and National Security letters from the US government requesting user information in the second half of 2016 as part of the company's semi-annual transparency report.

"In its semiannual transparency report, Apple reported that from July 1 to Dec. 31, 2016 it received 5,750-5,999 FISA orders and National Security Letters pertaining to 4,750-4,999 accounts.

Apple this week released its transparency report for the second half of 2016, revealing that U.S. government national security requests rose markedly from the previous six-month period."

26.05.17

The Hill

Tech giants urge Congress to revise foreign surveillance law

Major technology companies Facebook, Google and Microsoft have joined with other firms to lobby Congress to revise the existing US laws on foreign surveillance so that greater attention is paid to digital privacy.

"A coalition of technology companies that includes Facebook, Google and Microsoft is asking Congress to make changes to a foreign surveillance law.

In a Friday letter to House Judiciary Committee Chairman Bob Goodlatte(R-Va.), the companies urged the panel to revise Section 702 of the Foreign Intelligence Surveillance Act, which allows for intelligence agencies to spy on foreign nationals who are not on U.S. soil."

Internet Inclusion

No new items of relevance

Pan-Asia

Internet governance

31.05.17

Reuters

China says controversial cyber law not designed to cripple foreign firms

Ahead of its introduction this week the Chinese Government have issued a statement defending its controversial new cyber law, stating that its intention is not to impact the Chinese dealings of international businesses.

"China's top cyber authority said on Wednesday it is not targeting foreign firms with a controversial national cyber law set to come into effect on Thursday.

More than 50 overseas companies and business groups have lobbied against the law, which includes stringent data storage and surveillance requirements."

Cybersecurity

24.05.17

SC Media

Passwords may become passé in India

The Data Security Council of India has announced that it will look to abandon passwords as a security measure in favour of other technological tools currently under consideration.

"The Data Security Council of India (DSCI) is joining the movement away from using passwords as a security measure and will look to develop new authentication methods best suited for that nation.

To meet this goal the DSCI has partnered with the FIDO Alliance, which has established the FIDO India Working Group to come up with a solution, reported Data Breach Today. The group pointed to the Verizon 2017 Data Breach Report that found 81 percent of all breaches were due to weak, stolen or default passwords as the reason to find a new method to protect data."

26.05.17

MIS Asia

APT3 hackers linked to Chinese intelligence

A new report by Recorded Future has alleged that the APT3 hacker group has been operating in support of the Chinese Government's intelligence agency.

"The APT3 hacker group, which has been attacking government and defense industry targets since 2010, has been linked to the Chinese Ministry of State Security, according to a report by Recorded Future.

Other attackers have been linked to the Chinese military, but this is the first time a group has been connected to Chinese intelligence, said Samantha Dionne, senior threat analyst at Somerville, Mass.-based Recorded Future, Inc."

30.05.17

SC Media

Group IB fingers Lazarus as being behind recent SWIFT attacks

Russian cybersecurity company Group IB has announced in a new report what it feels is clear evidence that the Lazarus group of hackers were responsible for the cyberattacks on the SWIFT bank messaging services.

"The on-going whodunnit regarding cyberattacks on European financial firms through the SWIFT bank messaging services now has the Russian cybersecurity firm Group IB alleging North Korea, through the Lazarus group, is behind the attacks."

Privacy

No new items of relevance

Internet Inclusion

No new items of relevance

Rest of the World

Internet governance

No new items of relevance

Cybersecurity

25.05.17

SC Media

WannaCry patches mistakenly knock Aussie hospitals offline

Details have emerged indicating that in a bid to avoid the impact of the WannaCry ransomware attack five Australian hospitals have frozen staff members out of their computer systems through the improper installation of security patches.

"In a case of no good deed goes unpunished, five Australian hospitals accidently locked out staff access to the computer systems after installing patches designed to protect them from WannaCry ransomware."

31.05.17

CAJ News Africa

African Union unveils new cyber security guidelines

The African Union has unveiled a new set of cybersecurity guidelines which are hoped will better protect the continent from cyberattacks in the future that bare similarities to this month's WannaCry ransomware attack.

"The historic Internet Infrastructure Security Guidelines the Internet Society and African Union Commission have unveiled in Kenya are set to create a more secure internet infrastructure and change the way member countries approach cyber security preparedness.

A multi-stakeholder group of African and global internet infrastructure security experts has developed the guidelines."

Privacy

No new items of relevance

Internet Inclusion

31.05.17

The Guardian

Ethiopia turns off internet nationwide as students sit exams

Ethiopia's government has closed its citizen's access to the internet in a bid to prevent exam paper leaks that affected last years end of year exams for students in the 12th grade. This is the third time in the last 12 months that the government has suspended internet access.

"Ethiopia has shut off internet access to its citizens, according to reports from inside the country, apparently due leaked exam papers for the nation's grade 10 examinations.

Outbound traffic from Ethiopia was shutdown around 4pm UK time on Tuesday, according to Google's transparency report, which registered Ethiopian visits to the company's sites plummeting over the evening. By Wednesday afternoon, access still had not been restored."

31.05.17

HTXT

Number of South Africans with access to internet grows to 60%

South Africa's national statistics agency has found that 60% of South Africans now have access to the internet, an almost 6% increase on last year.

"Six out of 10 South Africans now has access to internet, an increase of 5.8% from last year, according to StatsSA.

StatsSA released its General Household Survey (GHS) 2016 survey today, which contains information on a variety of subjects including education, health, the labour market, dwellings, access to services and facilities, transport, and quality of life."

Global Institutions

26.05.17

ICANN

Empowered Community Power Triggered: Approval of Amendments to ICANN's Fundamental Bylaws

ICANN has provided further information on the next steps to be taken in amending the groups bylaws after it returned the approved list of amendments to the Empowered Community.

"On 23 May 2017, the ICANN organization sent a notice [PDF, 238 KB] to the Empowered Community that the ICANN Board has approved amendments to ICANN's Fundamental Bylaws to move the Board Governance Committee's reconsideration responsibilities to another Board Committee. This notice triggered a series of events that have been set in place for the Empowered Community to consider and approve the amendments before they can go into effect."

29.05.17

Digital Europe

DIGITALEUROPE submits response to ENISA/Commission consultation on ICT Security Certification

Digital Europe has published its response to the joint ENISA, EU Commission consultation on ICT security certification. In its submission the group indicated that greater attention be paid to the processes of security certification so as to retain flexibility in applying to products and services.

"On 19 May, DIGITALEUROPE submitted a response to the joint ENISA and European Commission consultation on ICT security certification. The consultation sought stakeholders views on a potential EU-wide ICT certification framework and a consumer based security labelling scheme."

Diary Dates

Modernising the regulations establishing the .eu top-level domain name – 05.05.17-04.08.17

European Commission

2017 European Security Conference – 05.06.17-06.06.17

Lisbon, Portugal

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

China Cyber Security Conference & Exposition 2017 – 13.06.17

Beijing, China

ICANN 59 – 26.06.17-29.06.17

Johannesburg, South Africa

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

ICANN 60 – 28.10.17-03.11.17

Abu Dhabi, United Arab Emirates

IGF 2017 – 18.12.17–21.10.17

Geneva, Switzerland