IEEE
GLOBAL INTERNET POLICY MONITOR
Read summaries of significant recent internet technology policy activities around the world

9 August 2017

Synopsis

Scroll to read full summaries with links to news articles.

The **UK** government has issued new **cybersecurity** guidelines to ensure manufacturers of smart **internet** connected vehicles better protect their products from cyber attacks.

A new report from **Ireland's** state-owned power grid suggests that the country has had its energy network compromised by **state sponsored hackers** after the **Vodafone** systems that support the network were found to have been breached.

Attila Peterfalvi, the head of **Hungary's** Data Protection Authority has criticised a lack of legal oversight in the Government's plans to centralise the **personal data** of Hungarian citizens.

In the **USA**, a number of State Governments have begun the process of strengthening their **cyber defences** for electoral systems ahead of the 2018 mid-term elections.

Illinois Governor **Bruce Rauner** has approved a new law that will now require all state employees to receive **cybersecurity awareness** training, making Illinois the 15th state to adopt the mandatory practice.

The **Chinese** Government has conducted a number of drills in conjunction with several **internet service providers** to test the country's ability to shut down websites deemed to be harmful to society.

India's Union Information Technology Minister **Ravi Shankar Prasad** has stated his ambition to develop an improved framework for the protection of **citizen data** within the country.

New research from **Research ICT Africa** has suggested that underlying issues relating **privacy** and **security** remain real barriers to internet use in Africa.

Digital Europe has championed a new campaign with national trade associations to ensure telecommunications ministers from each of the EU's member states abide by their previous commitments.

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

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

9 August 2017

Table of Contents

Europe

Internet governance

06.08.17

Reuters

UK government sets out tougher guidelines to protect smart cars from hackers

The UK government has issued new cybersecurity guidelines to ensure manufacturers of smart internet connected vehicles better protect their products from cyber attacks.

"The British government issued new guidelines on Sunday requiring manufacturers of internet-connected vehicles to put in place tougher cyber protections to ensure they are better shielded against hackers.

The government said it was concerned that smart vehicles, which allow drivers to do things such as access maps and travel information, could be targeted by hackers to access personal data, steal cars that use keyless entry systems, or take control of technology for malicious reasons."

08.08.17

SC Media

£17 million fines for CNI companies under proposed EU SNIS plans

As part of a new consultation from the Department for Digital, Culture, Media and Sport the UK Government has revealed that companies dealing in critical national infrastructure could face fines of £17million or 4% of their turnover for loss of services caused by cyber attacks.

"Under an (NIS) directive being adopted by the UK, CNI providers will face fines of £17 million or up to four percent of annual turnover if they fail to protect critical infrastructure from loss of services due to cyber-attacks.

Just as commercial companies must protect loss of customer data under EU GDPR or face huge fines, now electricity, water, energy, banking, financial markets, transport and health infrastructure providers will also face the same fines (£17 million or up to four percent of annual turnover) if they fail to protect critical infrastructure from loss of services due to cyber-attacks."

Cybersecurity

07.08.17

SC Media

Cyberattacks at sea prompt return of radio ship navigation

Due to the potential security risks posed by cyberattacks on the Global Positioning Systems of the worlds shipping fleets a number of countries have begun to develop analogue responses based on technology developed during World War II.

"The threat of possible cyberwarfare attacks against ships sea is prompting the return of navigators using radio navigation technology like Loran, as opposed, to modern GPS (Global Positioning System).

Building off of the quite old Loran (long-range navigation) system created during World War II, South Korea, the U.S., Britain and Russia are reportedly developing their own respective versions of an earth-based navigation technology known as eLoran, according to Reuters."

08.08.17

The Hill

Irish power grid compromised by foreign actor: report

A new report from Ireland's state-owned power grid suggests that the country has had its energy network compromised by state sponsored hackers after the Vodafone systems that support the network were found to have been breached.

"A foreign power compromised the cybersecurity of the state-owned Irish power grid company EirGrid, Ireland's Independent newspaper reports.

The report, issued Monday in Ireland, says that the telecommunications company Vodafone discovered last month that hackers had compromised its systems more than two months prior."

Privacy

07.08.17

Euractiv

[Hungary rights chief denounces 'data grab' bill]

Attila Peterfalvi, the head of Hungary's Data Protection Authority has criticised a lack of legal oversight in the Government's plans to centralise the personal data of Hungarian citizens.

"Hungary's data protection watchdog on Monday (7 August) lashed out at government plans to centralise personal data and ease rules on allowing official access, calling them a major threat to citizens' rights.

The bill, which was filed in parliament late last month, would lead to surveillance without any legal oversight, Attila Peterfalvi, head of the Hungarian Data Protection Authority (NAIH), told the station Klubradio."

07.08.17

Reuters

Britons will get right to delete online past, minister says

As part of the UK's implementation of the EU's General Data Protection Regulation the Government has confirmed that UK citizen's will be granted the right to be forgotten by social media platforms.

"Britons will be able to make social media platforms like Facebook (FB.O) delete information, including content published in their childhood, under government proposals that will bring data laws into line with new European regulations.

Individuals will have more control over their data by having "the right to be forgotten" and ask for their personal data to be erased in the measures announced by Digital Minister Matt Hancock on Monday."

Internet Inclusion

03.08.17

Out-Law

BT proposes to proactively fulfil UK government's goal of universal broadband

BT has volunteered to offer broadband access to all UK properties in a bid to avoid the implementation of a universal service obligation.

"The UK government is considering an offer from BT to provide universal broadband access to properties across the country in a move which could see a potential new regulatory universal service obligation (USO) for broadband scrapped.

The government has the power to introduce a new USO for broadband through provisions contained in the Digital Economy Act, which was introduced into UK law earlier this year. It has opened a consultation on how such an obligation could be designed, which builds on a report by Ofcom published late last year."

United States of America

Internet governance

No new items of relevance

Cybersecurity

06.08.17

The Hill

States ramping up defenses against election hacks

A number of State Governments have begun the process of strengthening their cyber defences for electoral systems ahead of the 2018 mid-term elections.

"States across the nation are ramping up their digital defenses to prevent the hacking of election systems in 2018.

The efforts come in the wake of Russia's interference in the 2016 presidential election, which state officials say was a needed wake up call on cybersecurity threats to election systems and infrastructure."

07.08.17

SC Media

Cyberattacks at sea prompt return of radio ship navigation

Due to the potential security risks posed by cyberattacks on the Global Positioning Systems of the worlds shipping fleets a number of countries have begun to develop analogue responses based on technology developed during World War II.

"The threat of possible cyberwarfare attacks against ships sea is prompting the return of navigators using radio navigation technology like Loran, as opposed, to modern GPS (Global Positioning System).

Building off of the quite old Loran (long-range navigation) system created during World War II, South Korea, the U.S., Britain and Russia are reportedly *developing their own respective versions of an earth-based navigation technology known as eLoran, according to Reuters."*

Privacy

07.08.17

SC Media

Disney sued, accused of violating child data privacy laws

The Disney corporation is facing a class action lawsuit following allegations that its gaming apps have allowed the capture and sale of the personal data of its child users.

"Disney was hit with a class action lawsuit for allegedly violating the Child Online Privacy Protection Act (COPPA) laws by capturing children's data and selling it to third parties.

The suit argues that Disney allows its technical partners including Upsight, Unity, Kochava, and other ad tech companies install proprietary code—so-called "software development kits" or SDKs—within Disney's gaming apps such as the Disney Princess Palace Pets app."

Internet Inclusion

04.08.17

Nextgov

FCC to spend billion to bring broadband to rural America

The FCC has announced plans to invest over $2billion in the next ten years on improving internet access for rural Americans through the wider provision of broadband services.

"Twenty-three million Americans don't have access to broadband internet, according to the Federal Communication Commission's 2016 Broadband Progress Report.

To help change these numbers, starting in 2018, the FCC plans to shell out $2 billion over the next decade to bring broadband access to more remote parts of the country."

08.08.17

The Hill

Illinois to require cybersecurity training for all state employees

Illinois Governor Bruce Rauner has approved a new law that will now require all state employees to receive cybersecurity awareness training, making Illinois the 15th state to adopt the mandatory practice.

“Illinois will now require cybersecurity awareness training for all state employees, thanks to legislation signed Monday.

"Cybersecurity is no longer just an IT issue. It is a public safety issue, and we will do all we can to protect the residents and infrastructure of our state, “said Gov. Bruce Rauner (R) at a press conference celebrating the new law.”

Pan-Asia

Internet governance

03.08.17

Reuters

China holds drill to shut down 'harmful' websites

The Chinese Government has conducted a number of drills in conjunction with several internet service providers to test the country’s ability to shut down websites deemed to be harmful to society.

“China held a drill on Thursday with internet service providers to practice taking down websites deemed harmful, as the country's censors tighten control ahead of a sensitive five-yearly political reshuffle set to take place later this year.

Internet data centers (IDC) and cloud companies - which host website servers - were ordered to participate in a three-hour drill to hone their "emergency response" skills, according to at least four participants that included the operator of Microsoft's cloud service in China.”

Cybersecurity

04.08.17

Networks Asia

1 in 3 Singapore SMEs victims of ransomware: study

A new report by Malwarebytes has found that over a third of small and medium sized businesses in Singapore have been the victim of ransomware.

“Ransomware is a relatively common problem for SMEs in Singapore, with more than one-third, 35%, of Singapore-based SMEs having experienced a ransomware attack in the last year, according to Malwarebytes' “Second Annual State of Ransomware Report.”

Close to a fifth (21%) of those who had been hit by ransomware had to cease all business operations immediately, and 11% lost revenue as a direct result of the attack.”

07.08.17

SC Media

Cyberattacks at sea prompt return of radio ship navigation

Due to the potential security risks posed by cyberattacks on the Global Positioning Systems of the worlds shipping fleets a number of countries have begun to develop analogue responses based on technology developed during World War II.

"The threat of possible cyberwarfare attacks against ships sea is prompting the return of navigators using radio navigation technology like Loran, as opposed, to modern GPS (Global Positioning System).

Building off of the quite old Loran (long-range navigation) system created during World War II, South Korea, the U.S., Britain and Russia are reportedly developing their own respective versions of an earth-based navigation technology known as eLoran, according to Reuters."

Privacy

04.08.17

First Post

Indian government is keen on formulating robust data protection laws

India's Union Information Technology Minister Ravi Shankar Prasad has stated his ambition to develop an improved framework for the protection of citizen data within the country.

Talking to reporters here, Prasad said "the country should have a framework that safeguards data properly and also enables its use for growth and development."

"As India has written a lot of discourse on internet governance the world over, I am very keen that India must come up with robust data protection laws that can become a beacon for the rest of the world," he said."

Internet Inclusion

No new items of relevance

Rest of the World

Internet governance

No new items of relevance

Cybersecurity

07.08.17

SC Media

Cyberattacks at sea prompt return of radio ship navigation

Due to the potential security risks posed by cyberattacks on the Global Positioning Systems of the worlds shipping fleets a number of countries have begun to develop analogue responses based on technology developed during World War II.

"The threat of possible cyberwarfare attacks against ships sea is prompting the return of navigators using radio navigation technology like Loran, as opposed, to modern GPS (Global Positioning System).

Building off of the quite old Loran (long-range navigation) system created during World War II, South Korea, the U.S., Britain and Russia are reportedly developing their own respective versions of an earth-based navigation technology known as eLoran, according to Reuters."

Privacy

07.08.17

SC Media

Australian Red Cross data breach caused by third-party error

The investigation into the 2016 Australian Red Cross data breach that revealed over half a million personal records has blamed a third-party company for creating a publicly available backup copy of the charity's blood donation website.

"An error by a third-party vendor's employee led to the massive data breach that hit the Australian Red Cross last year."

Internet Inclusion

03.08.17

IT Web Africa

Kenyans offline due to prohibitive costs, security fears

New research from Research ICT Africa has suggested that underlying issues relating privacy and security remain real barriers to internet use in Africa.

“Mozilla-backed research, carried out by Research ICT Africa, has revealed that Kenyans are offline due to prohibitive costs and security fears.

"While internet access is good in Kenya relative to elsewhere in Africa, real barriers remain to internet use. If we don't look beyond access issues to the real concerns around privacy and security, for example, we'll never bring the entire internet to all people," notes Research ICT Africa executive director, Alison Gillwald.”

Global Institutions

04.08.17

ICANN

ICANN61 Fellowship Application Round Now Open

ICANN has launched its fellowship application program ahead of the ICANN61 public meeting in March 2018, to be held in San Juan, Puerto Rico.

"Today, ICANN opened the Fellowship program application round for individuals interested in attending ICANN61. The Public Meeting takes place from 10–15 March 2018 in San Juan, Puerto Rico. The deadline to apply is 15 September 2017. Successful candidates will be announced on 1 December 2017 on https://icann.org/."

09.08.17

Digital Europe

DIGITALEUROPE is stepping up the role of being the leading Digital association in Europe.

Digital Europe has championed a new campaign with national trade associations to ensure telecommunications ministers from each of the EU's member states abide by their previous commitments.

"On 18 July 2017, telecom ministers from all European Member States gathered in Tallinn with a focus of attention to discuss the 5G policy, amongst other things.

We understood that the European Commission (EC) was discontented with the fact that the telecom ministers from the European Member States seemed to have been opting out on previous promises on alignment and investment towards a new European digital infrastructure."

Diary Dates

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

European Commission

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 – 18.12.17–21.12.17

Geneva, Switzerland