



**5 April 2017**

## Synopsis

**Scroll to read full summaries with links to news articles.**

**EU Commissioner Vera Jourova** has announced that the **EU-US Privacy Shield** will be reviewed in September as part of an ongoing process to ensure that the agreements central tenets are maintained.

In **Germany** this week the Country's **Cybersecurity** chief has announced that the German Army has suffered 284,000 separate **cyber attacks** in the first months of 2017.

**President Trump** has announced that the 2015 state of national emergency declared by Barack Obama following Russian interference in the US Presidential elections will be extended as "significant malicious **cyber-enabled activities**" continue to threaten the USA.

Following the Congressional repeal of **privacy** rules for internet service providers, major US ISPs **Comcast, Verizon** and **AT&T** have announced that they will not sell the browsing histories of their customers.

**Telstra's Cyber Security Report 2017** has found that 59% of **Asia** based businesses have experienced major **cybersecurity** breaches at least once a month. The study has also found that nearly 15% of businesses in **India** and **Hong Kong** experience major security incidents on a weekly basis.

**Hyderabad** has become the first **Indian** city with 1GBps **broadband**, increasing the city's already substantial **internet penetration**. Speaking at the announcement Government officials outlined plans for further expansion of WiFi hotspots.

A new program to increase **internet penetration** in rural areas has been announced by the **Rwandan** Government at the second Rwanda Internet for All Forum in Kigali. Amongst the programs intended goals are the creation of smart classrooms and greater public access to free WiFi.

**ICANN** have announced the results of the **ICANN58 Community Forum** survey which provides feedback on the ICANN58 meeting.

## IEEE Global Internet Policy Monitor

5 April 2017

### Table of Contents

<b>Synopsis .....</b>	<b>1</b>
<b>Europe .....</b>	<b>3</b>
Internet governance.....	3
Cybersecurity.....	3
Privacy.....	5
Internet Inclusion.....	5
<b>United States of America .....</b>	<b>6</b>
Internet governance.....	6
Cybersecurity.....	6
Privacy.....	8
Internet Inclusion.....	10
<b>Pan-Asia .....</b>	<b>11</b>
Internet governance.....	11
Cybersecurity.....	11
Privacy.....	11
Internet Inclusion.....	11
<b>Rest of the World.....</b>	<b>13</b>
Internet governance.....	13
Cybersecurity.....	13
Privacy.....	13
Internet Inclusion.....	14
<b>Global Institutions.....</b>	<b>15</b>
<b>Diary Dates.....</b>	<b>16</b>

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

## Europe

### Internet governance

*No new items of relevance*

### Cybersecurity

**03.04.17**

**SC Magazine**

#### [U.S., U.K. warn airports, nuclear facilities of cyberattacks](#)

The UK and US governments have issued warnings to national airports and nuclear facilities following concerns for a major cyberattack. In February the UK Government published its first warning to the Nuclear industry as part of the Civil Nuclear Cyber Security Strategy.

*“Airports and nuclear power plants in the U.S. and U.K. are on alert for cyberattacks after governments in both countries issued alerts.*

*In addition to intelligence that prompted the U.S. to ban laptops and other devices in passenger cabins of certain airlines to thwart terrorists attempting to bring explosives on board, the Telegraph [reported](#) that officials worried that bad actors might also attempt cyberattacks on airports and nuclear facilities.”*

**03.04.17**

**Politico**

#### [German cybersecurity chief: Army attacked over 284,000 times this year](#)

The German Army’s cybersecurity chief has announced that the German Army has suffered 284,000 separate cyber attacks in the first months of 2017 as he takes up his position in charge of a new cyber unit.

*“Computers belonging to the German army were attacked by hackers close to 300,000 times in the first few weeks of this year, Ludwig Leinhos, the new head of cyber command of the German army, told [Bild](#) Sunday.*

*Leinhos, who took charge of the German army’s cyber unit on Saturday, said that in future, wars could be won and lost online and Germany must prepare for the worst.”*

**04.04.17**

### **Air Transport World**

#### **[Two new European initiatives aim to improve aviation cybersecurity](#)**

Airbus CyberSecurity and SITA have combined their resources as part of a joint project to tackle cybersecurity issues in the aerospace industry, particularly for commercial travel. The new Security Operations Center Services will alert airlines and relevant stakeholders when potential cyber attacks are suspected.

*“Airbus CyberSecurity, a unit of Airbus Defense and Space, has joined forces with SITA to launch a [cybersecurity](#) initiative specifically targeted at the [air transport industry](#).”*

*The new incident-detection Security Operations Center Services have been customized for the specific needs of the air transport industry to alert airlines, airports, and other stakeholders about unusual cyber activity that could impact their businesses.”*

**05.04.17**

### **U.S. News & World Report**

#### **[UK and Swedish Watchdogs Warn of International Cyber Attack](#)**

The Swedish Civil Contingencies Agency and UK National Cyber Security Centre have identified in conjunction with PwC and BAE Systems that an international cyberattack has attempted to compromise systems potentially since 2014 by using IT services providers.

*“A large-scale cyber attack from a group targeting organizations in Japan, the United States, Sweden and many other European countries through IT services providers has been uncovered, the Swedish computer security watchdog said on Wednesday.”*

*The cyber attack, uncovered through a collaboration by Britain's National Cyber Security Centre, PwC and cyber security firm BAE Systems, targeted managed service providers to gain access to their customers' internal networks since at least May 2016 and potentially as early as 2014.”*

## Privacy

**04.04.17**

**SC Magazine**

### [EU commissioner announces September review for EU-US Privacy Shield](#)

EU Commissioner Vera Jourova has announced that the EU-US Privacy Shield will be reviewed in September as part of an ongoing process to ensure that the agreements central tenets are maintained.

*“Privacy Shield will be up for review in September. The date was announced by Vera Jourova, the European commissioner for justice, consumers and gender equality during a visit to Washington DC late last week.*

*She gave the speech on 31 March to the Center for Strategic and International Studies, a leading geopolitical thinktank. Jourova declared, “In a world where cross-border data flows have become a central feature of global trade, strong data protection rules would be meaningless if the data can travel abroad without protections.”*

## Internet Inclusion

**No new items of relevance**

## United States of America

### Internet governance

**No new items of relevance**

### Cybersecurity

**29.03.17**

**The Hill**

#### [White House extends Obama executive order on cyber threats](#)

President Trump has announced that the 2015 state of national emergency declared by Barack Obama following Russian interference in the US Presidential elections will be extended as “significant malicious cyber-enabled activities” continue to threaten the USA.

*“President Trump will continue a 2015 state of national emergency that President Obama used as a basis for freezing the assets of Russians tied to a hacking campaign aimed at disrupting the presidential election.*

*In a letter to Congress titled “Message to the Congress Regarding the Continuation of the National Emergency with Respect to Significant Malicious Cyber-Enabled Activities,” Trump renewed the order signed in April 2015. The executive order would have expired without renewal.”*

**29.03.17**

**NextGov**

#### [Nist Cyber Framework for Federal Agencies coming soon](#)

The National Institute of Standards and Technology has announced that its Cybersecurity Framework for Federal agencies is nearing completion. The Trump administration is believed to be considering instating the NIST framework as a mandatory requirement for Federal agencies as part of an Executive Order on cybersecurity.

*“The government’s cyber standards agency is nearing completion on a document that will help federal agencies integrate a cybersecurity framework developed for industry with government’s own particular cybersecurity requirements, an official said Wednesday.*

*Expect the document in the next two months or perhaps sooner, said Matthew Barrett, program manager for the National Institute of Standards and Technology's Cybersecurity Framework.”*

**31.03.17**

**The Hill**

**[WikiLeaks' latest leak shows how CIA avoids antivirus programs](#)**

This week has seen WikiLeaks release a further set of documents allegedly from the CIA that outlines how the espionage agency bypasses antivirus programs to allow the agency to plant malware on devices.

*“WikiLeaks released its third package of CIA documents on Friday which highlight source code used by the CIA to avoid antivirus programs.*

*The source code is for a tool called "Marble," what is known as an obfuscator or packer.*

*Obfuscators are principally designed to jumble the execution of malware so that programs designed to spot malware have trouble determining what it is.”*

**03.04.17**

**SC Magazine**

**[U.S., U.K. warn airports, nuclear facilities of cyberattacks](#)**

The UK and US governments have issued warnings to national airports and nuclear facilities following concerns for a major cyberattack. In February the UK Government published its first warning to the Nuclear industry as part of the Civil Nuclear Cyber Security Strategy.

*“Airports and nuclear power plants in the U.S. and U.K. are on alert for cyberattacks after governments in both countries issued alerts.*

*In addition to intelligence that prompted the U.S. to ban laptops and other devices in passenger cabins of certain airlines to thwart terrorists attempting to bring explosives on board, the Telegraph [reported](#) that officials worried that bad actors might also attempt cyberattacks on airports and nuclear facilities.”*

**04.04.17**

### **Daily Energy Insider**

#### **[Lawmakers broaden scrutiny of cybersecurity across U.S. energy delivery systems](#)**

The Senate Energy and Natural Resources Committee has expanded its inquiry into the cybersecurity of the US energy system to include natural gas, having previously conducted session focused only on the electricity grid.

*“Federal lawmakers on Tuesday expanded their examination of how well the U.S. electric grid is protected against cybersecurity threats to include the efforts of defending the nation’s natural gas pipelines against cyber terror.*

*“Given the interdependency of natural gas and electricity, it is imperative that these energy delivery systems are adequately protected” against the increasing number of cyberattacks, said U.S. Sen. Lisa Murkowski (R-AK), chairman of the Senate Energy and Natural Resources Committee, which held a hearing on the topic.”*

### **Privacy**

**31.03.17**

### **Reuters**

#### **[Major internet providers say will not sell customer browsing histories](#)**

Following the Congressional repeal of privacy rules for internet service providers, major US ISPs Comcast, Verizon and AT&T have announced that they will not sell the browsing histories of their customers.

*“Comcast Corp, Verizon Communications Inc and AT&T Inc said Friday they would not sell customers’ individual internet browsing information, days after the U.S. Congress approved legislation reversing Obama administration era internet privacy rules.*

*The bill would repeal regulations adopted in October by the Federal Communications Commission under former President Barack Obama requiring internet service providers to do more to protect customers’ privacy than websites like Alphabet Inc’s Google or Facebook Inc.”*

**03.04.17**

**Digital Journal**

**[Verizon slammed for installing 'spyware' on phones](#)**

The telecommunications company Verizon has been criticised by the Electronic Frontier Foundation for appearing to install spyware on new phones. The criticism came after the EFF analysed the privacy policy of Verizon's new app AppFlash and found that it could be used for targeted advertising.

*"Verizon has been accused of installing "spyware" on new phones. The company has developed an app that's supposed to help people find content from services they don't have installed. The privacy policy reveals it does more than make recommendations.*

*The app is called AppFlash and it was announced last week. It will be available on Android phones sold by Verizon as a new launcher tab available to the left of the home screen. Once fully operational, it'll include links to nearby restaurants, movies for you to watch and details of news apps to download."*

**04.04.17**

**New York Daily News**

**[New York high court sides with Manhattan DA after Facebook challenged warrant for user data](#)**

The Court of Appeals in New York has rejected an appeal by Facebook against the bulk seizure of user data through search warrants. However the Court's ruling was specific as it only enforced the precedent that search warrants are not appealed, rather than ruling on the collection of data in bulk.

*"New York's highest court punted Tuesday on a challenge by Facebook of bulk seizure of users' accounts by Manhattan District Attorney Cy Vance.*

*The Court of Appeals ruled 5-1 that while the case "undoubtedly implicates novel and important substantive issues regarding the constitutional rights of privacy and freedom from unreasonable search and seizure," its authority was limited."*

**04.04.17**

## **SC Magazine**

### **[EU commissioner announces September review for EU-US Privacy Shield](#)**

EU Commissioner Vera Jourova has announced that the EU-US Privacy Shield will be reviewed in September as part of an ongoing process to ensure that the agreements central tenets are maintained.

*“Privacy Shield will be up for review in September. The date was announced by Vera Jourova, the European commissioner for justice, consumers and gender equality during a visit to Washington DC late last week.*

*She gave the speech on 31 March to the Center for Strategic and International Studies, a leading geopolitical thinktank. Jourova declared, “In a world where cross-border data flows have become a central feature of global trade, strong data protection rules would be meaningless if the data can travel abroad without protections.”*

## **Internet Inclusion**

***No new items of relevance***

## Pan-Asia

### Internet governance

*No new items of relevance*

### Cybersecurity

03.04.17

**Security Asia**

#### [Cyber security attacks on the rise in Asia; India, HK most at risk](#)

Telstra's Cyber Security Report 2017 has found that 59% of Asia based businesses have experienced major cybersecurity breaches at least once a month. The study has also found that nearly 15% of businesses in India and Hong Kong experience major security incidents on a weekly basis.

*"More than half of organizations (59 per cent) surveyed in Asia have detected a business interrupting security breach at least once a month, shows the Cyber Security Report 2017 released by Telstra.*

*The study paints a mixed view of the state of cyber security in Asia, most alarming is the increase and regularity of cyber-attacks on businesses, while cloud security came up as a major security issue for Asian organisations."*

### Privacy

*No new items of relevance*

### Internet Inclusion

31.03.17

**The New Indian Express**

#### [Hyderabad becomes first 'Giga-enabled' city in India](#)

Hyderabad has become the first Indian city with 1GBps broadband, increasing the city's already substantial internet penetration. Speaking at the announcement Government officials outlined plans for further expansion of WiFi hotspots.

*“With the launch of 1 GBPS wired broadband internet connection here on Thursday, Hyderabad has become the first ‘Giga-enabled’ city in India.*

*“Hyderabad is the city with highest internet penetration in India. With launch of the net connection, it has now become the first Giga City in the country and is on par with cities like Hong Kong and Singapore. Hyderabad is home to a buzzing IT industry, start-up culture, industries, students and 1 GBPS net connection will be of great use for the people,” said IT and Municipal Administration minister KT Rama Rao, after launching the connection. ACT (Atria Convergence Technologies) Fibrenet, a Hyderabad-based company, which is a leading internet service provider in the country, has launched the connection.”*

## Rest of the World

### Internet governance

**No new items of relevance**

### Cybersecurity

**05.04.17**

**IT Web Africa**

#### [Calls for Ghana to serve as cybercrime fighting hub](#)

An international workshop hosted by the Council of Europe and National Communications Authority has called on Ghana to act as a regional training centre for Anglophone West Africa to improve regional responses to cybercrime.

*“At an international workshop on criminal justice statistics on cybercrime and electronic evidence, where the potential increase in cybercrime was discussed, a representative of the Council of Europe has called on Ghana to act as a regional hub for cybercrime training within Anglophone West Africa.*

*According to Matteo Lucchetti, whose CoE organised the event with National Communications Authority, Ghana can promote the adoption of international standards in the neighbouring countries based on the view that Ghana represents a best practice in the region on matters related to cybercrime and cyber-enabled crimes.”*

### Privacy

**No new items of relevance**

## Internet Inclusion

**03.04.17**

**New Times (Rwanda)**

### [New programme to accelerate internet access in rural areas](#)

A new program to increase internet penetration in rural areas has been announced by the Rwandan Government at the second Rwanda Internet for All Forum in Kigali. Amongst the programs intended goals are the creation of smart classrooms and greater public access to free WiFi.

*“Internet penetration in rural areas is expected to grow thanks to a programme dubbed “Smart village” that was launched in Kigali, during the second edition of Rwanda Internet for All Forum.*

*The forum, which was held in Kigali on Friday, was organised by the Ministry of Youth and ICT in collaboration with the World Economic Forum.”*

## Global Institutions

**03.04.17**

**ICANN**

### [ICANN Releases Results of ICANN58 Survey](#)

ICANN has published the results of its ICANN58 Community Forum Survey, as part of procedures to assess ICANN's ability to meet the needs of attendees to global meetings.

*“On 3 April 2017, ICANN published the findings of the ICANN58 Community Forum survey. At the end of every ICANN Public Meeting, we ask participants to rate the sessions, facilities, networking opportunities and format of the meeting.*

*Our goal is to improve the data we collect, and to look for trends by comparing meeting data over time. This information gives us greater insights into how we are meeting the needs of attendees, and informs the kinds of changes we need to make.”*

## Diary Dates

[Building the European data economy](#) – 10.01.17-26.04.17

[ENISA evaluation and review](#) – 18.01.17 – 12.04.17

[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