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

## 6 September 2017

## Synopsis

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

**Andrus Ansip**, the European Commission's Vice President in charge of digital issues has criticised **CERT** teams across the **EU**, saying that only half are truly capable of defending their national networks. His comments, come days before the expected publication of a raft of new EU **cybersecurity** proposals.

President of the **International Cyber Threat Task** Force (ICCTF) **Paul C Dwyer**, has called on the **UK** and **Irish** governments to form a special task force to deal with the **cybersecurity** issues facing Irish citizens as part of the UK's termination its of EU membership.

The **UK** Government have launched a new industry survey with which it hopes to better understand the specialist **digital skills** required in the UK's digital economy.

The US **Food and Drug Administration** has recalled 500,000 **pacemakers** over concerns that **cybersecurity** vulnerabilities could lead to the death of users.

**Democrats** in the Senate are to fight a proposal by the **FCC** to redefine what constitutes **broadband internet access**, claiming that the regulator is trying to lower standards so it can more easily meet existing targets.

**India** and the **EU** have reaffirmed their joint commitment to a free and secure **cyberspace** following the fourth iteration of the **India-EU Cyber Dialogue**.

Indian telecoms regulator **TRAI** has again confirmed that it expects to finalise the recommendations for its proposals on **Net Neutrality** within the next month.

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

## 6 September 2017

## Table of Contents

Synopsis ........ 1

Europe ........ 4
- Internet governance ........ 4
- Cybersecurity ........ 5
- Privacy ........ 6
- Internet Inclusion ........ 6

United States of America ........ 7
- Internet governance ........ 7
- Cybersecurity ........ 7
- Privacy ........ 8
- Internet Inclusion ........ 8

Pan-Asia ........ 9
- Internet governance ........ 9
- Cybersecurity ........ 9
- Privacy ........ 10
- Internet Inclusion ........ 10

Rest of the World ........ 11
- Internet governance ........ 11
- Cybersecurity ........ 11
- Privacy ........ 11
- Internet Inclusion ........ 11

Global Institutions ........ 12

Diary Dates ........ 13

# Europe

## Internet governance

**31.08.17**

**The Indian Express**

**India, EU reaffirm commitment to free, secure cyberspace**

India and the EU have reaffirmed their joint commitment to a free and secure cyberspace following the fourth iteration of the India-EU Cyber Dialogue.

*"India and the European Union (EU) reaffirmed their commitment to a free and secure cyberspace during the fourth India-EU Cyber Dialogue held here on Tuesday, the External Affairs Ministry said on Wednesday. "India and EU reaffirmed their commitment to an open, free, secure, stable, peaceful and accessible cyberspace, enabling economic growth and innovation," the Ministry said in a statement."*

**06.09.27**

**Euractiv**

**Ansip vows to respect 'sovereignty' with new cyber security measures**

Andrus Ansip, the European Commission's Vice President in charge of digital issues has criticised CERT teams across the EU, saying that only half are truly capable of defending their national networks. His comments, come days before the expected publication of a raft of new EU cybersecurity proposals.

*"One week before the European Commission is expected to present a slew of new cyber security proposals, Vice-President Andrus Ansip said that the new measures will not take away too much power from EU countries' national authorities.*

*"We respect the sovereignty of our member states but we know that maybe in 50% of member states those national CERTs are not so able to protect networks," Ansip said on Tuesday (5 September), referring to CERTs, or national units that respond to cyber security incidents."*

## Cybersecurity

**01.09.17**

**Reuters**

**Norway tightens IT security to prevent ballot tampering**

The Norwegian govenrment has moved to enforce stricter security for its electoral mechanism ahead of parliamentary elections next week. Improvements to existing cybersecurity measures have also been included in the upgraded security.

*“Norway is tightening security procedures ahead of a parliamentary election on Sept. 11 to prevent possible vote tampering, the government said on Friday.*

*The security of IT systems will be enhanced, and all votes must be counted manually at least once in addition to the customary scanning of ballot papers by computers, it added.”*

**04.09.17**

**Irish Times**

**Call for Anglo-Irish task force to deal with post-Brexit cyber security**

President of the International Cyber Threat Task Force (ICCTF) Paul C Dwyer, has called on the UK and Irish governments to form a special task force to deal with the cybersecurity issues facing Irish citizens as part of the UK’s termination its of EU membership.

*“Ireland and Britain need to form a cyber task force to deal with the fallout from the Brexit negotiations, which are “clearly failing to address the concerns of the digital community and digital borders on matters relating to cyber security and data protection”, an Irish expert has said.*

*President of the International Cyber Threat Task Force (ICCTF)* Dwyer said *the Brexit discussions had so far been “light on detail regarding any implications or solutions for cyber security and data protection”.”*

**06.09.17**

**Reuters**

**EU looks to extra spending, diplomacy to bolster cyber security**

As part of the European Commission's upcoming range of proposals for increased cybersecurity cooperation in the European Union, the Commission is expected to focus on shared investment to improve cybersecurity standards across the bloc.

*"The European Commission wants to bolster cyber security in the EU by increasing investment in technology, setting stricter consumer safeguards and stepping up diplomacy to deter attacks by other nations, among other measures.*

*The Commission is due to announce its proposals in a report later this month, a copy of which was obtained by Reuters on Wednesday. It also argues for greater national and law enforcement cooperation to halt incoming attacks."*

## Privacy

***No new items of relevance***

## Internet Inclusion

**31.08.17**

**Computer Weekly**

**UK Government launches digital skills survey to find out more about UK's needs**

The UK Government have launched a new industry survey with which it hopes to better understand the specialist digital skills required in the UK's digital economy.

*"The government wants to better understand the UK's specialist digital skills needs, and has launched a survey to gather information.*

*The digital skills and inclusion team at the Department for Digital, Culture, Media and Sport (DCMS) has launched the study to find out more about the UK's digital workforce, and to determine what the characteristics of an advanced or specialist digital workforce are."*

# United States of America

## Internet governance

***No new items of relevance***

## Cybersecurity

**31.08.17**

**The Guardian**

**Hacking risk leads to recall of 500,000 pacemakers due to patient death fears**

The US Food and Drug Administration has recalled 500,000 pacemakers over concerns that cybersecurity vulnerabilities could lead to the death of users.

*"Almost half a million pacemakers have been recalled by the US Food and Drug Administration (FDA) due to fears that their lax cybersecurity could be hacked to run the batteries down or even alter the patient's heartbeat.*

*The recall won't see the pacemakers removed, which would be an invasive and dangerous medical procedure for the 465,000 people who have them implanted: instead, the manufacturer has issued a firmware update which will be applied by medical staff to patch the security holes."*

**05.09.17**

**The Hill**

**Senate Dem pushes for government-wide ban of Russian cyber firm**

Democratic Senator Jeanne Shaheen has called on the US Government to ban the use of software produced by Kaspersky lab due to concerns for the company's connections with Russian intelligence services.

*"Sen. Jeanne Shaheen (D-N.H.) is pushing for a government-wide ban of security software produced by a Russian-origin cyber firm on the grounds that the company's "extensive ties to Russian intelligence" threaten the United States.*

*Shaheen has already successfully introduced an amendment to the Senate's version of annual defense policy legislation that would bar the Defense Department from using Kaspersky Lab software. But the Democratic senator wants the final bill to go even further, by instituting a ban on all federal agencies from using software produced by the company."*

## Privacy

**05.09.17**

**SC Media**

**Lenovo settles privacy charges with FTC, 32 states**

Lenovo has settled a privacy suit with the FTC and 32 state authorities after MitM software on its computers compromised the privacy of consumers.

*"Lenovo has settled privacy charges with the Federal Trade Commission and attorney generals in 32 states stemming from man-in-the-middle (MitM) software pre-installed on it consumer laptops.*

*The VisualDiscovery software created "serious security vulnerabilities" for those laptop users because it served as a MitM between and even encrypted websites, allowing the software program access to consumers' personal information, including Social Security numbers, medical information, financial and payment information and login credentials, the FTC said."*

## Internet Inclusion

**05.09.17**

**Ars Technica**

**Senate Democrats fight FCC plan to lower America's broadband standards**

Democrats in the Senate are to fight a proposal by the FCC to redefine what constitutes broadband internet access, claiming that the regulator is trying to lower standards so it can more easily meet existing targets.

*"Senate Democrats are fighting a Federal Communications Commission proposal that could lower America's broadband standards by redefining what counts as broadband Internet access."*

# Pan-Asia

## Internet governance

**31.08.17**

**The Indian Express**

**India, EU reaffirm commitment to free, secure cyberspace**

India and the EU have reaffirmed their joint commitment to a free and secure cyberspace following the fourth iteration of the India-EU Cyber Dialogue.

*"India and the European Union (EU) reaffirmed their commitment to a free and secure cyberspace during the fourth India-EU Cyber Dialogue held here on Tuesday, the External Affairs Ministry said on Wednesday. "India and EU reaffirmed their commitment to an open, free, secure, stable, peaceful and accessible cyberspace, enabling economic growth and innovation," the Ministry said in a statement."*

## Cybersecurity

**31.08.17**

**Reuters**

**Chinese cyber spies broaden attacks in Vietnam, security firm says**

Researchers from cybersecurity company FireEye have provided new analysis alleging that China's cyber espionage workers have turned their attentions on corporations and government officials in Vietnam.

*"Cyber spies working for or on behalf of China's government have broadened attacks against official and corporate targets in Vietnam at a time of raised tension over the South China Sea, cyber security company FireEye said.*

*FireEye told Reuters the attacks happened in recent weeks and it had traced them back to suspected Chinese cyber spies based partly on the fact that a Chinese group it had identified previously had used the same infrastructure before."*

**01.09.17**

**Defense World**

**Indian Govt Finalizing Cyber Security Standards For Mobile Companies**

The Indian government has announced that it is in the final stages of its planning ahead of the introduction of a wave of new cybersecurity standards for mobile devices in a bid to improve consumer protections against cyberattacks.

*"Indian government is finalising cyber security standards to counter rising cyber attacks and breach of financial and personal data from mobile-phone companies.*

*"The products of all mobile manufacturing units must be security-compliant. There will be no compromise on this issue," Union Minister for Information Technology and Electronics Ravi Shankar Prasad is quoted as saying at a summit on cyber and network security by various local media Thursday."*

## Privacy

**No new items of relevance**

## Internet Inclusion

**31.08.17**

**Indian Express**

**TRAI Net Neutrality decision next month, but telecos spar with Internet firms**

Indian telecoms regulator TRAI has again confirmed that it expects to finalise the recommendations for its proposals on Net Neutrality within the next month.

*"Telecom regulator TRAI today said it is likely to finalise recommendations on net neutrality, which calls for access to internet content without any discrimination in data speed and cost with telecom and internet firms sparring over the controversial issue. Telecom operators have been pushing for their right to charge for content like video and commercial websites as per the business case so that they have more funds to invest in building telecom infrastructure."*

# Rest of the World

## Internet governance

***No new items of relevance***

## Cybersecurity

**04.09.17**

**SC Media**

**Pacifier APT backdoor components have suspected ties to Russia-linked Turla Group**

Researchers from cybersecurity firm Bitdefender have alleged in a new whitepaper that Russian linked Turla Group has been responsible for a number of cyberattacks on government instituions based on the Pacifier AP backdoor vulnerability.

*"Bitdefender researchers spotted three new Pacifier APT backdoor components that appear to connect the group's cyber-espionage campaigns against government institutions to the Russia-linked Turla Group.*

*Researchers spotted new components that communicate with command and control servers using three very innovative techniques, one of which is a binary that can communicate with a command and control server (C&C) by proxying the connection through an internet-connected computer that shares the same LAN as the victim, according to a recent Whitepaper."*

## Privacy

***No new items of relevance***

## Internet Inclusion

***No new items of relevance***

# Global Institutions

**31.08.17**

**ICANN**

**Webinar: "Statistical Analysis of DNS Abuse in gTLDs" (SADAG) Study**

ICANN are to hold a webinar to discuss the findings of the organisation’s SADAG study on the safeguards of the new gTLD program.

*“The Internet Corporation for Assigned Names and Numbers (ICANN) today announced that they will host an interactive webinar entitled, "The Statistical Analysis of DNSAbuse in gTLDs" (SADAG). The webinar is based on a study commissioned by the Competition, Consumer Trust and Consumer Choice Review Team (CCTRT) as part of its examination of consumer trust and effectiveness of safeguards that were built into the New Generic Top-Level Domain (gTLD) Program.”*

# Diary Dates

**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